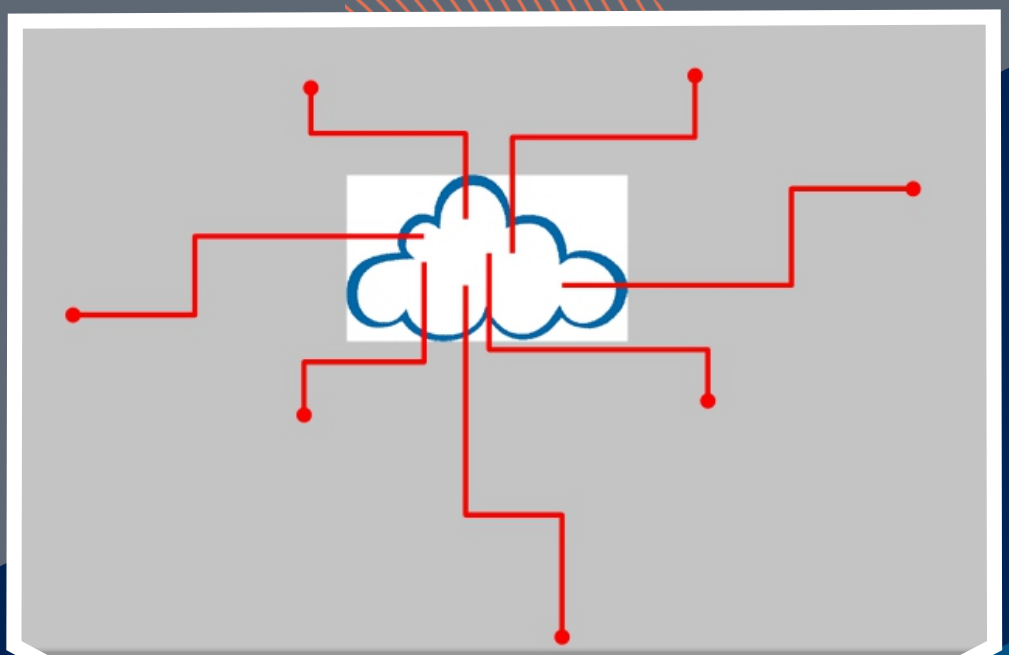
Grzegorz Owczarek, Artur Hłobaż

OCHRONA DANYCH OSOBOWYCH I ZAPEWNIENIE CYBERBEZPIECZEŃSTWA W SYSTEMACH INTELIGENTNYCH ŚRODKÓW OCHRONY INDYWIDUALNEJ



CIOP PIB

Materiały informacyjne CIOP-PIB
Ochrona danych osobowych i zapewnienie cyberbezpieczeństwa w systemach inteligentnych środków ochrony indywidualnej

Opracowano na podstawie wyników IV etapu programu wieloletniego „Poprawa bezpieczeństwa i warunków pracy" finansowanego w latach 2017-2019 w zakresie zadań służb państwowych przez Ministerstwo Rodziny, Pracy i Polityki Społecznej.

Koordynator programu: Centralny Instytut Ochrony Pracy – Państwowy Instytut Badawczy.

Zadanie 3.G.05: Opracowanie wytycznych do ochrony danych osobowych i cyberbezpieczeństwa w systemach inteligentnych środków ochrony indywidualnej

Autorzy:
dr inż. Grzegorz Owczarek – Centralny Instytut Ochrony Pracy – Państwowy Instytut Badawczy, Zakład Ochron Osobistych, Pracownia Ochron Oczu i Twarzy
dr inż. Artur Hłobaż – Uniwersytet Łódzki, Wydział Fizyki i Informatyki Stosowanej

Okładka: Jolanta Maj

CIOP PIB
Centralny Instytut Ochrony Pracy – Państwowy Instytut Badawczy
ul. Czerniakowska 16, 00-701 Warszawa
tel. (48-22) 623 36 98, www.ciop.pl

Spis treści

Wprowadzenie

W czasie, w którym powstawał niniejszy poradnik, niemal cały świat komentował wydarzenia związane z wyciekiem danych z najbardziej popularnego serwisu społecznościowego[1]. Komentatorzy, naukowcy, a także zwykli użytkownicy Internetu zastanawiali się, czy ich dane, które znalazły się w zasobach Facebooka, nie wyciekły? Jeśli tak, to kto mógł je wykraść i do jakich celów mogły zostać wykorzystane? Serwisy społecznościowe to jeden z wielu obszarów, w których są gromadzone dane wprowadzane przez samych użytkowników. Wcale nie musimy jednak mieć konta na serwisie społecznościowym lub własnego adresu poczty elektronicznej, aby dane, które mogą posłużyć do naszej identyfikacji, mogły zostać przechwycone, a w konsekwencji kontrolowane i wykorzystane przez niepowołane osoby. Czasami nie zdajemy sobie nawet sprawy, że użytkując wiele urządzeń elektronicznych, identyfikujemy się z nimi i chcąc nie chcąc, sami stajemy się częścią globalnego Internetu, a właściwie to Internetu rzeczy (ang. *Internet of Things*, IoT), czyli przestrzeni, w której różnego rodzaju przedmioty, wyposażone w czujniki oraz moduły do transmisji danych, mogą komunikować się ze sobą i wymieniać dane za pośrednictwem sieci komputerowej. Współczesny świat oferuje nam wiele urządzeń, których sposobu działania – niestety musimy się chyba do tego przyznać? – nie do końca rozumiemy. Zafascynowani możliwościami współczesnej elektroniki i informatyki stajemy się posiadaczami urządzeń, które mogą zbierać różnego rodzaju informacje, w tym również te, które mają charakter wrażliwy (np. dane osobowe, o stanie zdrowia i miejscu przebywania itp.). Brzmi to dość zaskakująco, ale zapewne wielu z nas spotkało się choćby z takim zdarzeniem, że ktoś, kto wcale nas fizycznie nie śledził, poinformował nas np. o tym, gdzie byliśmy w danym dniu i jak długo trwała nasza wycieczka rowerowa. Wybierając się na wycieczkę rowerową, zabieramy ze sobą smartfona z funkcją lokalizacji GPS (ang. *global position system*) lub zakładamy urządzenie do monitorowania aktywności fizycznej, czyli tzw. opaskę typu *fitness*. Wtedy – oczywiście pod warunkiem że urządzenia te są aktywne – dane o naszym położeniu lub monitorowanych parametrach fizjologicznych zostają wysłane do chmury obliczeniowej[2]. Oczywiście dostęp do nich jest szyfrowany. Problem jednak polega na tym, że każda metoda służąca do zabezpieczania danych może przecież zostać złamana. Nigdy nie możemy mieć pewności,

[1] W marcu 2018 r. miała miejsce głośna afera związana z firmą Cambridge Analytical i Facebookiem. Z doniesień medialnych wynikało, że wyciekły dane nawet 50 mln użytkowników Facebooka na całym świecie.
[2] Chmurą obliczeniową określamy model przetwarzania danych. Model ten zwykle oparty jest na użytkowaniu określonych usług dostarczonych przez usługodawcę, czyli podmiot zarządzający chmurą obliczeniową.

że dane zbierane z wykorzystaniem użytkowanych przez nas urządzeń elektronicznych, które funkcjonują w przestrzeni określanej jako IoT, są stuprocentowo bezpieczne.

Stosowanie urządzeń elektronicznych funkcjonujących w przestrzeni IoT dotyczy również środowiska pracy, w którym coraz powszechniejsze jest stosowanie systemów inteligentnych środków ochrony indywidualnej. Za bezpieczeństwo w miejscu pracy odpowiedzialność ponosi przede wszystkim pracodawca. To do jego obowiązków należy organizacja stanowiska pracy oraz wyposażenie pracownika w niezbędne na danym stanowisku środki eliminujące lub minimalizujące ryzyko związane z występowaniem określonych zagrożeń. **Jeśli więc na stanowisku pracy pojawiają się urządzenia lub systemy zdolne do pozyskiwania, gromadzenia oraz przetwarzania danych, wśród których mogą znaleźć się także dane o charakterze wrażliwym, obowiązkiem pracodawcy jest również zapewnienie ochrony tych danych.** Różnorodność technologii zastosowanych do konstrukcji urządzeń i systemów, które służą do pozyskiwania, gromadzenia oraz przetwarzania danych w środowisku pracy, sprawia, że zagadnienie zapewnienia cyberbezpieczeństwa i ochrony danych jest bardzo szerokie. **Niniejszy poradnik ma na celu zwrócenie uwagi zarówno na zagadnienia prawnej ochrony danych osobowych, jak i na wybrane aspekty stosowanych technologii. Jest on przeznaczony dla wszystkich osób zainteresowanych funkcjonowaniem innowacyjnych technologii w środowisku pracy.**

Część poradnika poświęcona zagadnieniom technologicznym dedykowana jest skierowana głównie do konstruktorów oraz osób konfigurujących na stanowiskach pracy wszelkiego rodzaju urządzenia i systemy inteligentnych środków ochrony indywidualnej, wyposażone w czujniki oraz moduły do transmisji danych oraz zabezpieczenia transmisji danych. W tej części opisano m.in. przykłady istniejących systemów oraz scharakteryzowano technologie i standardy stosowane do transmisji danych, ze wskazaniem na zagrożenia związane z bezpieczeństwem danych. Sformułowano również najważniejsze zalecenia w zakresie zapewnienia cyberbezpieczeństwa i ochrony danych.

Część poradnika poświęcona ochronie danych w świetle obowiązujących przepisów jest skierowana głównie do osób, które pełnią w firmie obowiązki administratora danych. Zgodnie z Rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie ich swobodnego przepływu oraz uchylenia dyrektywy 95/46/WE (Dziennik Urzędowy UE L 119/1 z 4 maja 2016) w Polsce w maju 2018 r. zostały wprowadzone nowe uregulowania prawne w zakresie ochrony danych.

1. Internet rzeczy

W rozdziale scharakteryzowano koncepcję IoT. W tej koncepcji dowolne elementy wyposażone w czujniki mogą gromadzić, wysyłać lub przetwarzać dane za pośrednictwem sieci komputerowej.

Gdy w 1999 r. cały świat – w tym Polska[3] – bardzo starannie przygotowywał się na nadejście pluskwy milenijnej, która miała sparaliżować działanie pojedynczych komputerów oraz sieci komputerowych z uwagi na przyjęty sposób zapisu daty, Kevin Ashton po raz pierwszy użył określenia IoT. Przedstawił **koncepcję, która zakłada, że określone przedmioty mogą pośrednio lub bezpośrednio pozyskiwać, gromadzić, wysyłać lub przetwarzać dane za pośrednictwem sieci (głównie sieci komputerowej)**[4].

Pomimo upływu prawie dwudziestu lat od sformułowania koncepcji IoT oraz bardzo dużej liczby publikacji na ten temat do tej pory brakuje jednoznacznej definicji IoT[5]. Jednym ze sposobów na określenie koncepcji IoT jest wyłącznie odzwierciedlenie sytuacji, w której wraz z rozwojem techniki, głównie Internetu oraz technologii wytwarzania sensorów, rośnie liczba połączonych ze sobą inteligentnych produktów (ang. *smart products*)[6]. W tym podejściu Internet obejmuje zasięgiem również obiekty fizyczne, które mogą się ze sobą komunikować. Internet, jako technologia, jest więc obszarem, w którym znajduje się również miejsce dla inteligentnych produktów, a to miejsce określa się jako IoT.

Innym podejściem jest osadzenie koncepcji IoT w maszynach oraz innych obiektach fizycznych wyposażonych w sensory oraz urządzenia inicjujące określone działania (aktuatory). W tym podejściu to połączone ze sobą obiekty fizyczne wyznaczają nowe obszary funkcjonowania Internetu. Do tych obszarów należy zaliczyć m.in.: gromadzenie danych, zdalne monitorowanie, algorytmy wspomagające podejmowanie decyzji, optymalizację różnorodnych procesów itp.[7].

[3] Informacja o wynikach działań administracji publicznej w celu minimalizacji „Problemu Roku 2000" dla funkcjonowania strefy publicznej w Polsce, Najwyższa Izba Kontroli, Departament Administracji i Integracji Europejskiej, 222/1999.
[4] Ashton K.: *That 'Internet of Things' Thing* [online]. RFID JOURNAL [dostęp: 2018-02-15]. http://www.rfidjournal.com/articles/view?4986
[5] Wielki J.: *Internet Rzeczy i jego wpływ na modele biznesowe współczesnych organizacji gospodarczych*, Zeszyty Naukowe Uniwersytetu Ekonomicznego w Katowicach 2016, nr 281, s. 2018-2019.
[6] Heppelmann J., Porter M.: *How to Smart, Connected Products Are Transforming Competition*, Harvard Business Review 2014, November.
[7] Dobbs R. et al.: *No Ordinary Disruption*. New York, Public Affairs 2015.

Niezależnie od kierunku, z którego zostanie wypracowana definicja IoT, koncepcja ta jest oparta na czterech podstawowych elementach:

- przedmiotach wyposażonych w czujniki i aktuatory;
- sieci komputerowej, która łączy przedmioty;
- systemach, które przesyłają i przetwarzają dane;
- modułach (np. aplikacje komputerowe) służących do tworzenia informacji i wnioskowania.

Aby można było mówić o IoT, muszą koniecznie współistnieć wszystkie wymienione powyżej elementy. Wynika to z tego, iż same przedmioty wyposażone nawet w najbardziej zaawansowane technologicznie czujniki i aktuatory bez możliwości łączenia się (sieci komputerowe) oraz bez możliwości przesyłania i przetwarzania danych (systemy przesyłające i przetwarzające dane) nie będą mogły funkcjonować w przestrzeni internetowej. Z kolei funkcjonowanie w przestrzeni internetowej obiektów fizycznych niegenerujących żadnych informacji, do wytworzenia których są niezbędne odpowiednie aplikacje, jest bezcelowe.

Cele, które są stawiane urządzeniom działającym w odniesieniu do koncepcji IoT, odzwierciedlają cztery podstawowe funkcjonalności, określające sposób przeznaczenia i wykorzystania tych urządzeń[8]:

- monitorowanie,
- kontrola,
- optymalizacja,
- autonomia.

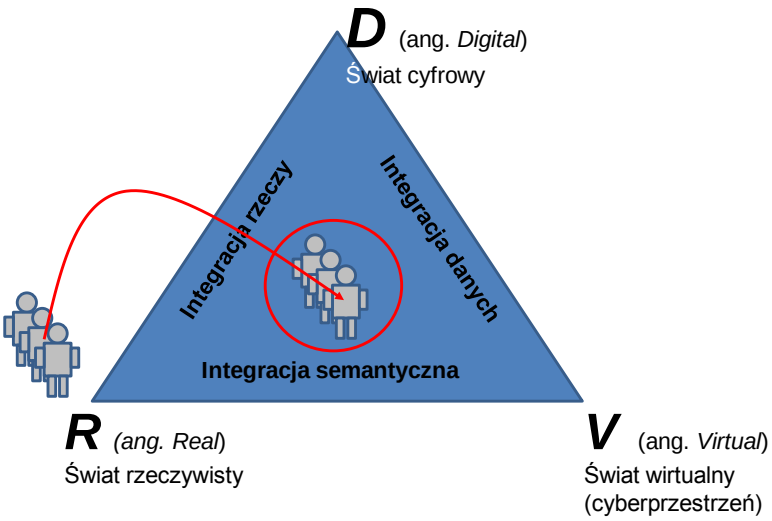
Pierwsze z dwóch wymienionych funkcjonalności są wynikiem zastosowania czujników dołączonych do obiektów fizycznych. Dzięki zastosowaniu aktuatorów oraz modułów służących do tworzenia informacji i wnioskowania można znacząco poprawić funkcjonowanie obiektów fizycznych. Możliwość monitorowania, kontrolowania oraz optymalizacji może z kolei zapewnić autonomię działania w stopniu niemożliwym do osiągnięcia bez wzajemnego współdziałania wszystkich elementów, na których opiera się koncepcja IoT.

Internet rzeczy jest więc koncepcją, która zakłada współistnienie określonych elementów oraz definiuje założone funkcjonalności. Może być więc rozumiana jako ekosystem, w którym przedmioty komunikują się między sobą za pośrednictwem człowieka lub bez jego udziału. W ekosystemie tym wyróżnia się następujące główne obszary zastosowania[9]:

[8] Wielki J.: *Internet Rzeczy i jego wpływ* [...], op.cit.
[9] Vermesan O., Friess P.: *Internet of Things – From Research and Innovation to Market Deployment* [online]. River Publishers 2014 [dostęp: 2019-04-17]. http://www.internet-of-things-research.eu/pdf/IERC_Cluster_Book_2014_Ch.3_SRIA_WEB.pdf

- środowisko i gospodarka wodna,
- przemysł i produkcja,
- transport i energia,
- miasta, budynki i mieszkania,
- zdrowie i życie.

Internet rzeczy to także koncepcja, która łączy świat rzeczywisty ze światem wirtualnym i cyfrowym. Integracja tych trzech światów jest możliwa dzięki połączeniu ze sobą rzeczy, czyli różnego rodzaju obiektów fizycznych (integracja rzeczy) funkcjonujących w świecie rzeczywistym przez dane (integracja danych), które można otrzymać w procesie funkcjonowania tych rzeczy/obiektów. Podstawę tej integracji stanowi relacja pomiędzy zbiorem pojęć świata rzeczywistego i wirtualnego (integracja semantyczna). Graficznym przedstawieniem integracji świata rzeczywistego ze światem wirtualnym i cyfrowym jest trójkąt *RVD* (ang. *Real, Virtual, Digital*) przedstawiony na rysunku 1[10].

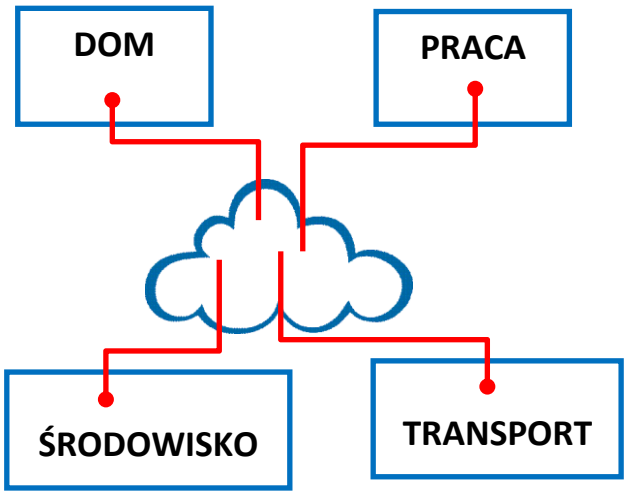


Rys. 1. Graficzne przedstawienie koncepcji łączącej świat rzeczywisty ze światem wirtualnym i cyfrowym[11]

W dużym uproszczeniu, elementy, które mogą pozyskiwać, gromadzić, wysyłać lub przetwarzać dane za pośrednictwem sieci komputerowej, a więc elementy IoT, mogą funkcjonować we wszystkich obszarach naszego życia, czyli w domu, w pracy, podczas podróży oraz gdziekolwiek byśmy nie przebywali. Właściwie istnieje tylko jeden warunek. Musi być dostęp do sieci kompute-

[10] Owczarek G.: *Wybór czujników do monitorowania parametrów środowiska pracy i zdrowia pracowników*. W: *Nowe trendy w bezpieczeństwie pracy, środowisku i zarządzaniu*. Pod red. nauk. B. Szczuckiej-Lasoty & W. Kriesera. Katowice, Wyższa Szkoła Zarządzania Ochroną Pracy 2018.
[11] Opracowano na podstawie: *Internet of things, strategic research roadmap* [online]. DOCPLAYER [dostęp: 2019-04-17]. https://docplayer.net/11937485-Internet-of-things-strategic-research-roadmap-antoine-de-saint-exupery.html

rowej, dzięki której jest możliwa łączność pomiędzy tymi urządzeniami. Sytuację tę przedstawiono schematycznie na rysunku 2.



Rys. 2. Obszary funkcjonowania elementów IoT (materiały własne autorów)

Twórca koncepcji IoT zapewne nie przypuszczał, jak duża będzie liczba urządzeń, których działanie można wpisać w przedstawioną przez niego koncepcję. Liczba sprzedawanych na świecie urządzeń, które działają w odwołaniu do tej koncepcji, charakteryzuje się wyraźną tendencją wzrostową. Zgodnie z przewidywaniami firmy Gartner, Inc.[12] globalna sprzedaż urządzeń IoT w roku 2050 będzie na poziomie 25 mld sztuk, co oznacza ponad ośmiokrotny wzrost w stosunku do liczby tych urządzeń sprzedanych w roku 2013 (ok. 3,0 mld)[13]. Konkretne dane związane z udziałem urządzeń mobilnych na rynku podają również firmy zajmujące się bezpośrednią sprzedażą tych urządzeń. Dla przykładu firma Apple informuje, że w roku 2014 sprzedała 28,8 mln inteligentnych urządzeń wykorzystywanych do monitoringu aktywności dziennej i parametrów życiowych, a w roku 2015 liczba sprzedanych urządzeń tego typu wyniosła aż 78,1 mln[14].

[12] Gartner, Inc. – założone w 1979 r. w Stanach Zjednoczonych przedsiębiorstwo analityczno-doradcze specjalizujące się w zagadnieniach strategicznego wykorzystania technologii oraz zarządzania technologiami.
[13] Dane: Gartner, Inc., listopad 2014.
[14] Dane na podstawie: DOBREPROGRAMY [dostęp: 2018-02-15]. https://www.dobreprogramy.pl/macminik/Rynek-mobilnych-gadzetow-sie-rozwija,70723.html

2. Bezpieczeństwo obiegu danych i informacji w systemach Internetu rzeczy

W rozdziale zdefiniowano pojęcie danych i informacji, omówiono podstawowe zasady, na których opiera się obieg danych w systemach IoT, oraz przedstawiono warstwową strukturę bezpieczeństwa danych.

2.1. Dane i informacje

Pisząc o obiegu danych i informacji w różnego rodzaju systemach elektronicznych, należy w pierwszej kolejności określić, co kryje się pod pojęciem „dane"? Internetowy słownik pojęć technicznych[15] definiuje dane jako **wszelkiego rodzaju informacje, które przygotowane są w celu przetworzenia, przechowywania lub przesyłania**. Mogą to być różnego typu pliki lub strumienie danych multimedialnych (np. VOD, czyli ang. *Video on Demand*, radio internetowe itp.), dane pomiarowe z czujników, dane uwierzytelniające (głównie login i hasło), strony internetowe, poczta elektroniczna itp. Z punktu widzenia przechowywania oraz przesyłania danych przez sieć komputerową stanowią one ciąg bitów. Dopiero na poziomie warstwy aplikacji jest on interpretowany ze względu na zawartość, tzn. co ten ciąg bitów reprezentuje i jakiego rodzaju są dane[16].

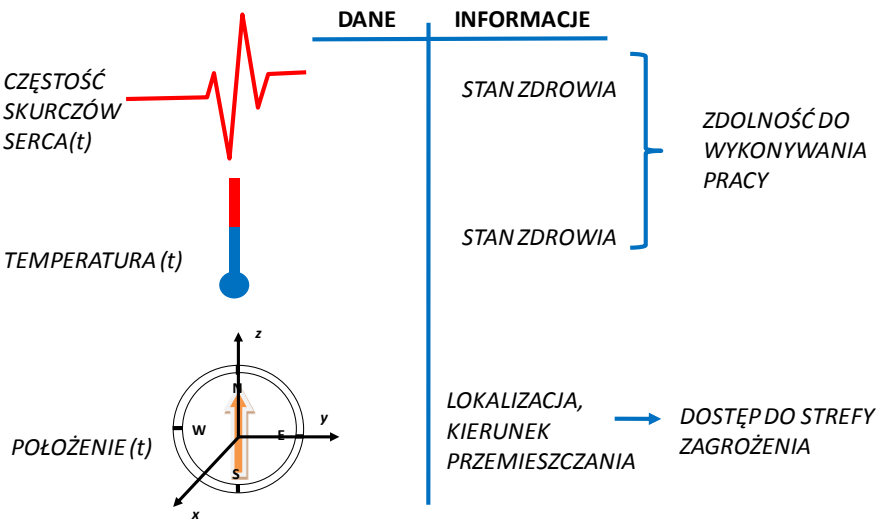
Dane definiowane są również jako zbiory liczb i tekstów o różnych formach. Mogą więc mieć konkretną wartość informacyjną[17]. Semantyczna różnica pomiędzy pojęciami „dane" a „informacje" polega na tym, że różne dane mogą dostarczać tę samą informację, ale jednocześnie te same dane mogą dostarczać różnych informacji. Takie rozróżnienie obu pojęć, czyli założenie że do otrzymania informacji niezbędne jest pozyskanie określonych danych, przedstawiono schematycznie na rysunku 3[18].

[15] Na podstawie internetowego słownika pojęć technicznych „TechTerms", TechTerms [dostęp: 2018-05-10]. https://techterms.com/definition/data [hasło: data]

[16] Na podstawie serwisu internetowego Computer Hope", Computer Hope [dostęp: 2018-05-10]. https://www.computerhope.com/jargon/d/data.htm

[17] Wilson G.: *Przetwarzanie danych dla programistów*. [Tł. M. Pętlicki]. Gliwice, Wydawnictwo HELION 2006.

[18] Owczarek G.: *Wybór czujników do monitorowania parametrów środowiska pracy i zdrowia pracowników*. W: *Nowe trendy w bezpieczeństwie pracy, środowisku i zarządzaniu*. Pod red. nauk. B. Szczuckiej-Lasoty & W. Kriesera. Katowice, Wyższa Szkoła Zarządzania Ochroną Pracy 2018.



Rys. 3. Uzyskiwanie informacji z pozyskanych danych (materiały własne autorów)

W zaprezentowanym na rysunku 3 przykładzie częstość skurczów serca, temperatura oraz położenie są rejestrowane w czasie. Na podstawie tych danych można uzyskać informacje o stanie zdrowia, lokalizacji oraz kierunku przemieszczania się pracownika. Przekładają się one z kolei na informacje o zdolności do wykonywania pracy oraz ewentualnym dostępie pracownika do strefy zagrożenia.

Z uwagi na możliwość zróżnicowania pojęć „dane" i „informacje" w dalszej części poradnika, podczas omawiania zagadnień w odniesieniu do architektury bezpieczeństwa IoT, jest stosowane wyłącznie określenie „dane". W części, w której opisano przykłady systemów środowiska pracy, rozróżniono pojęcia „danych" i otrzymywanych na ich podstawie „informacji".

2.2. Dlaczego należy zapewnić bezpieczeństwo obiegu danych i informacji?

Jedną z najważniejszych przesłanek do monitorowania bezpieczeństwa w obiegu danych i informacji w cyberprzestrzeni są ataki hakerskie. Cyberprzestrzeń – w tym również cyberprzestrzeń środowiska pracy – podlega ciągłemu narażeniu na ingerencję osób nieuprawnionych[19]. Problem ten stał się obecnie nie tylko problemem technicznym, lecz również zagadnieniem szeroko dyskutowanym pod kątem zachowań społecznych. Powszechnie znane jest już określenie

[19] Mitnick K., Simon W. L.: *Ghost in the Wires. My Adventures as the World's Most Wanted Hacker*. Boston, Little, Brown and Company 2011.

„haker" – zaczerpnięte ze slangu komputerowego – czyli osoby o bardzo dużej wiedzy i umiejętnościach z zakresu systemów informatycznych, niestety wykorzystywanych głównie do łamania zabezpieczeń systemów komputerowych. Hakerzy są obecnie traktowani jako swego rodzaju subkultura, do której zalicza się również inne, wyspecjalizowane w atakach na określone obszary cyberprzestrzeni, grupy, takie jak np.: machinisci, scenowcy i fanfikowcy, hejterzy, cyberpanki i cybergoci[20]. Jeśli podczas ataków hakerskich zostaną przechwycone dane osobowe, a więc dane o charakterze wrażliwym, a następnie zostaną one wykorzystane niezgodnie z intencjami osób, których dotyczą, może to być powodem wielu zdarzeń, których skutki nie zawsze są do końca przewidywalne. Mogą to być skutki ekonomiczne, prawne lub osobowe (związane choćby z narażeniem konkretnej osoby na ujawnienie w przestrzeni publicznej informacji o jej stanie zdrowia itp.). Kolejnym, niemniej ważnym powodem, dla którego konieczne jest monitorowanie bezpieczeństwa danych, są wymogi prawne.

2.3. Obieg danych i architektura bezpieczeństwa w systemach IoT

Obieg danych we wszystkich systemach elektronicznych i telekomunikacyjnych, bankowych itp., a także w przestrzeni określanej jako IoT jest oparty na trzech podstawowych elementach:

- integralność,
- poufność,
- dostępność.

Integralność oznacza, że zebrane dane są kompletne i wystarczająco dokładne, aby wygenerować informacje, które chcemy otrzymać. Należy również zapewnić odpowiednie metody przetwarzania tych danych. **Poufność** oznacza, że zebrane dane/informacje są dostępne jedynie dla osób do tego upoważnionych. **Dostępność** to zapewnienie osobom upoważnionym dostępu do danych/informacji zawsze, gdy jest taka potrzeba[21].

Przykładem, który doskonale obrazuje obowiązywanie zasad integralności, poufności i dostępności, są powszechnie użytkowane systemy bankowe. Kompletność danych, do których mają dostęp klienci banków, polega m.in. na wygenerowaniu przez system informacji o znajdującej się na ich koncie kwocie (z odpowiednią dokładnością) oraz nazwie podmiotu, który przelał lub wpłacił na konto klienta banku określoną kwotę. Zapewnienie odpowiednich metod przetwarzania to

[20] Kałdon B.: *Cyberprzestrzeń jako zagrożenie dla człowieka XXI wieku*. SEMINARE 2016, t. 37, nr 2, s. 87-101.
[21] Stallings W.: *Cryptography and Network Security. Principles and Practice*. Pearson Education Limited, London 2016.

w tym przypadku np. możliwość wykonywania przez klienta przelewów, płatności itp. Dostęp do danych widocznych na koncie danego klienta banku ma on sam oraz w szczególnych przypadkach – co jest regulowane przez ścisłe procedury prawne – inne upoważnione osoby. W celu zapewnienia poufności stosuje się odpowiednie metody logowania i uwierzytelniania dostępu. Warunkiem dostępności do danych bankowych, których dotyczy omawiany przykład, jest oczywiście również dostęp do urządzeń technicznych, np. laptopy i smartfony z dostępem do Internetu. Na przykładach systemów bankowych doskonale widać ogromny postęp w obszarze obiegu danych. Interfejsy użytkowników (w omawianym przykładzie klientów banku) oraz sposoby korzystania z własnych zasobów zdeponowanych w banku są nieustannie rozwijane. Można więc powiedzieć, że w tym przypadku w pełni obowiązuje zasada integralności, czyli zapewnienia dokładności i kompletności danych oraz optymalnych metod przetwarzania. Zastosowanie wielu metod weryfikacji dostępu to w tym przypadku zapewnienie zasady poufności, a możliwość dostępu do danych o koncie z poziomu smartfona to wypełnienie zasady dostępności, czyli zapewnienie, że osoby upoważnione mają dostęp do danych/informacji i związanych z nimi aktywami zawsze, gdy jest im to potrzebne. Zdarza się jednak, że nawet najbardziej zaawansowane pod względem bezpieczeństwa systemy bankowe są narażone na wyciek danych i przechwycenie ich przez osoby nieupoważnione, czego konsekwencją mogą być straty dla klientów lub samego banku.

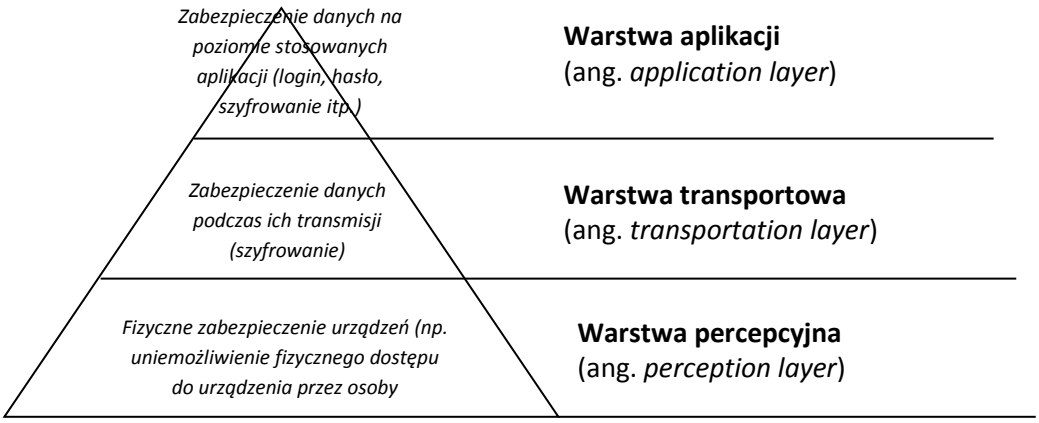
Wśród przyczyn, które mogą doprowadzić do takiej sytuacji, wymienia się:

- brak właściwej architektury bezpieczeństwa,
- błędy w zarządzaniu bezpieczeństwem informacji,
- błędy oprogramowania,
- błędy i/lub celowe działanie człowieka,
- niewystarczające monitorowanie bezpieczeństwa.

Najlepszą metodą zabezpieczania danych jest metoda wielopoziomowa odnosząca się m.in. zarówno do bezpieczeństwa fizycznego, jak i do aplikacji. Ogólny schemat architektury bezpieczeństwa (patrz rysunek 4) dla wszystkich systemów w obszarze IoT może składać się z trzech podstawowych warstw[22]:

- percepcyjnej,
- transportowej,
- aplikacji.

[22] Qi Jing, Vasilakos A. V., Wan J., Jingwei Lu, Dechao Qiu: *Security of the Internet of Things: perspectives and challenges*. Wireless Networks 2014, vol. 20, issue 8, s. 2481-2501.



Rys. 4. Warstwowa architektura bezpieczeństwa IoT i elementy zabezpieczenia poszczególnych warstw (materiały własne autorów)

Na każdej z warstw przedstawionych na rysunku 4 zabezpieczanie danych może odbywać się niezależnie. Ta niezależność jest niezmiernie istotna z punktu widzenia bezpieczeństwa całego systemu[23]. Przykładowo, jeśli dane będą zabezpieczone tylko podczas transmisji (zabezpieczenie w warstwie transportowej), nadal będzie istniała możliwość uzyskania do nich dostępu dzięki dostępowi do niezabezpieczonego urządzenia (brak zabezpieczenia w warstwie aplikacji na poziomie laptopa lub smartfona). Podobnie jeśli dostęp do danych zgromadzonych w urządzeniu będzie zabezpieczony (zabezpieczenie w warstwie aplikacyjnej), to można uzyskać do nich dostęp w trakcie ich przesyłania za pomocą sieci w postaci niezaszyfrowanej (brak zabezpieczenia w warstwie transportowej). Brak niezależności w zabezpieczaniu danych w poszczególnych warstwach tworzących architekturę systemów IoT jest niezmiernie istotnym elementem wpływającym na bezpieczeństwo danych. Zabezpieczenie danych w warstwie percepcyjnej odnosi się do fizycznego zabezpieczenia urządzeń, które służą do zbierania danych (np. czujniki) oraz ich przechowywania (komputery, smartfony itp.).

Struktura wielowarstwowa, w której dane są zabezpieczone niezależnie na każdym poziomie, daje szansę na ochronę danych przed atakami skierowanymi na przełamanie metod zabezpieczeń wykorzystanych w każdej z warstw. Mechanizmy silnego uwierzytelnienia, zastosowanie mocnych protokołów szyfrowania oraz zabezpieczenie danych na poziomie aplikacji to warunki konieczne do zapewnienia cyberbezpieczeństwa. Nigdy nie ma jednak pełnej gwarancji, że osoby nieuprawnione nie uzyskają dostępu do danych.

[23] Surman G.: *Understanding security using the OSI Model*. Swansea, SANS Institute. Information Security Reading Room 2002 [dostęp: 2019-04-17]. https://www.sans.org/reading-room/whitepapers/protocols/understanding-security-osi-model-377

Zaprezentowana trójwarstwowa architektura bezpieczeństwa IoT stanowi jedną z możliwych. Możliwe jest bardziej szczegółowe rozdzielenie poszczególnych warstw, tak aby wyodrębnić najważniejsze elementy wchodzące w skład danego systemu. Przykład to struktura pięciowarstwowa, składająca się z[24]:

- warstwy percepcyjnej (ang. *perception layer*),
- warstwy bezpieczeństwa i kontekstu (ang. *security and context layer*),
- warstwy sieciowej i transportowej (ang. *network and transportation layer*),
- warstwy chmurowej (ang. *cloud storage and mobility*),
- warstwy analitycznej (ang. *analytical layer*).

Warstwowa struktura bezpieczeństwa IoT jest w dużej mierze zbieżna ze standardem OSI (ang. *Open Systems Interconnection Reference Model*) opisującym ogólną strukturę komunikacji sieciowej[25]. Standard ten składa się z siedmiu warstw: fizycznej, łącza danych, sieciowej, transportowej, sesji, prezentacji i aplikacji.

[24] Na podstawie: Mehta R.: *Why Industrial IoT platform is best hope for IT and OT convergence* [online]. CIO [dostęp: 2019-04-17]. https://www.cio.com/article/2977651/predictive-analytics/why-industrial-iot-platform-is-best-hope-for-it-and-ot-convergence.html

[25] Standard opracowany w latach dziewięćdziesiątych XX wieku przez ISO (Międzynarodową Organizację Normalizacyjną) oraz ITU-T (Sektor Normalizacji i Telekomunikacji).

3. Technologie i standardy stosowane do transmisji danych w systemach IoT

W rozdziale opisano powszechnie stosowane technologie do transmisji danych w systemach IoT. Wyjaśniono zasadę działania danej technologii oraz wskazano na zagrożenia związane z bezpieczeństwem danych, co jest kluczowe w przypadku zapewnienia cyberbezpieczeństwa w systemach inteligentnych środków ochrony indywidualnej, takich jak systemy monitorowania stanu zdrowia i/lub warunków pracy.

3.1. Zestaw standardów do budowy sieci bezprzewodowych Wi-Fi

Zasada działania Wi-Fi

Technologia Wi-Fi to jedna z najbardziej powszechnie stosowanych technologii bezprzewodowych działająca w dwóch zakresach: 2,4 GHz (pasmo częstotliwości: od 2400 do 2485 MHz) oraz 5 GHz (pasmo częstotliwości: od 4915 do 5825 MHz). Określana jest również jako zestaw standardów z rodziny IEEE 802.11. W dzisiejszych czasach ma dwa główne zastosowania. Pierwsze z nich polega na jej wykorzystywaniu przy budowie bezprzewodowych sieci lokalnych WLAN (ang. *Wireless Local Area Network*) opartych na komunikacji radiowej, z czym najczęściej można się spotkać w domu, szkole lub firmie. Drugi wariant zastosowań dotyczy budowania, np. w miastach, przez dostawców usług internetowych ISP (ang. *Internet Service Provider*) rozległych sieci bezprzewodowych WWAN (ang. *Wireless Wide Area Network*), dzięki czemu użytkownicy wyposażeni w przenośne urządzenia zgodne z Wi-Fi mają bezprzewodowy dostęp do sieci.

W zależności od zastosowanych urządzeń i standardu można uzyskiwać różne odległości i przepustowości/szybkości łączności bezprzewodowej. Poniżej przedstawiono zestawienie najpowszechniej obecnie stosowanych standardów sieci bezprzewodowych z rodziny IEEE 802.11[26]:

- Standard B (802.11b) – standard, który jest rozszerzeniem oryginalnego standardu 802.11. Obsługuje przepustowość do 11 Mb/s i wykorzystuje częstotliwość 2,4 GHz. Maksymalny zasięg w budynku – do 30 m.

[26] Mitchell B.: *802.11 Standards Explained: 802.11ac, 802.11b/g/n, 802.11a* [online]. Lifewire [dostęp: 2019-04-23]. https://www.lifewire.com/wireless-standards-802-11a-802-11b-g-n-and-802-11ac-816553

- Standard G (802.11g) – obsługuje przepustowość do 54 Mb/s i wykorzystuje częstotliwość 2,4 GHz. Jest wstecznie kompatybilny z 802.11b, co oznacza, że punkty dostępowe 802.11g będą działać z bezprzewodowymi kartami sieciowymi 802.11b i na odwrót. Maksymalny zasięg w budynku – do 35 m.
- Standard N (802.11n) – standard, w którym po raz pierwszy wprowadzono opcjonalne wykorzystanie pasma 5 GHz i 2,4 GHz razem. W wersji n również po raz pierwszy wprowadzono zastosowanie anten MIMO (ang. *Multiple Input, Multiple Output*) dla większej równoległej przepustowości. W zależności od liczby połączeń antenowych szybkość przesyłu mogą teoretycznie osiągnąć do 750 Mb/s – dla standardu N750. Maksymalny zasięg w budynku – do 50 m.
- Standard AC (802.11ac) – wersja standardu Wi-Fi, który został zaprojektowany w celu znacznego zwiększenia szybkości przesyłania danych. Jest to pierwszy standard w kierunku opracowania „Gigabit Wi-Fi", w którym szybkość przesyłanych danych może osiągnąć do 1 Gbit/s. Standard ten działa w paśmie 5 GHz, co umożliwia uzyskanie większych szybkości w porównaniu ze standardami 802.11n lub g działającymi na 2,4 GHz. Maksymalny zasięg w budynku – do 35 m.

Zestawienie najpowszechniej obecnie stosowanych standardów sieci bezprzewodowych z rodziny IEEE 802.11 przedstawiono na rysunku 5.

Rys. 5. Zestawienie najpowszechniej obecnie stosowanych standardów sieci bezprzewodowych z rodziny IEEE 802.11[27]

Zagrożenia bezpieczeństwa danych w systemach Wi-Fi

Tak jak inne technologie bezprzewodowe sieć Wi-Fi również może być narażona na różnego rodzaju ataki i zagrożenia. W związku z tym że najpopularniejsze standardy Wi-Fi w większości

[27] Dziedzic K.: *Wi-Fi bez tajemnic* [online]. Komputer Świat [dostęp: 2019-04-23]. http://www.komputerswiat.pl/jak-to-dziala/2015/06/standardy-wifi.aspx

przypadków wykorzystują pasmo 2,4 GHz, z którego korzystają również inne urządzenia, jak: telefony komórkowe, kuchenki mikrofalowe, Bluetooth, to transmisja danych może zostać zagłuszona lub mieć ograniczony zasięg. Również w przypadku konfiguracji punktów dostępowych sieci bezprzewodowej AC (ang. *Access Point*) należy zawsze pamiętać o ich poprawnym skonfigurowaniu. W przypadku braku lub niepoprawnej konfiguracji urządzenie to może stać się celem ataku. Do zabezpieczenia transmisji przesyłanych danych należy również wybierać najmocniejszy z możliwych protokołów. Obecnie najmocniejszym z możliwych wariantów jest WPA2, który wykorzystuje mocne mechanizmy szyfrowania, w tym m.in. algorytm kryptograficzny AES[28].

3.2. Technologia transmisji danych krótkiego zasięgu RFID

Zasada działania RFID

RFID (ang. *Radio Frequency Identification*) jest jedną z najpopularniejszych technologii krótkiego zasięgu wykorzystywanych do transmisji danych. Do zbioru tych danych należą głównie dane pozwalające na identyfikację obiektów, na których są umieszczane znaczniki. Do przesyłania danych oraz zasilania znaczników wykorzystuje się pole elektromagnetyczne o częstotliwości radiowej. Systemy posługujące się technologią RFID składają się z dwóch zasadniczych elementów:

- znacznika (określanego również tagiem lub etykietą), umieszczanego na identyfikowanym obiekcie;
- czytnika, którego rolą jest głównie odczytanie zawartych w znaczniku danych.

Dane odczytane przez czytniki mogą być przesyłane do komputera i analizowane z wykorzystaniem dowolnych aplikacji.

Znaczniki RFID

Znacznik RFID jest zbudowany z pamięci i anteny. Jego wygląd i budowa zależy m.in. od zakresu częstotliwości radiowej.

[28] *Security Labs. Wszystko o cyberbezpieczeństwie. Gdzie czają się niebezpieczeństwa? Jak ochronić siebie, swoje urządzenie i swoją tożsamość?* [online]. GData Security Labs [dostęp: 2019-05-30]. https://www.gdata.pl/security-labs,bezpieczenstwo-sieci-bezprzewodowych

Z uwagi na częstotliwość znaczniki dzieli się na:

- znaczniki niskich częstotliwości LF (ang. *low frequency*), pracujące na częstotliwościach od 125 do 134 kHz;
- znaczniki wysokich częstotliwości HF (ang. *high frequency*), pracujące na częstotliwości 13,56 MHz;
- znaczniki ultra wysokich częstotliwości UHF (ang. *ultra high frequency*), pracujące na częstotliwościach od 860 do 960 MHz.

Schemat obrazujący zasięg, wygląd oraz najważniejsze obszary zastosowania znaczników RFID w zależności od częstotliwości pracy znacznika przedstawiono na rysunku 6.

Rys. 6. Schemat obrazujący zasięg, wygląd oraz najważniejsze obszary zastosowania znaczników RFID w zależności od częstotliwości pracy znacznika (materiały własne autorów)

Innym rodzajem podziału znaczników **jest podział ze względu na sposób zasilania lub ze względu na możliwość zapisu w nich danych**. W przypadku pierwszej kategorii podziału rozróżniamy znaczniki aktywne, które mają własne źródło zasilania, oraz znaczniki pasywne, bez źródła zasilania. W przypadku drugiej kategorii wyróżniamy następujące typy znaczników:

- tylko do odczytu (ang. *Read Only*) – informacje w znaczniku są zapisywane w trakcie jego produkcji,
- jednokrotnego zapisu i wielokrotnego odczytu, tzw. WORM (ang. *Write Once, Read Many*) – pozwalają na jednorazowe ustawienie danych identyfikacyjnych,
- wielokrotnego zapisu i odczytu RW (ang. *Read – Write*) – umożliwiające użytkownikowi zapisywanie, modyfikowanie i usuwanie własnych danych.

Znaczniki zaopatrzone są na ogół w pamięć od 64 do 128 bitów, chociaż można spotkać również takie, których pojemność pamięci przekracza 64 kB. W przypadku standardowego zastosowania (głównie identyfikacja) wystarczająca jest pamięć rzędu kilkuset bitów.

Czytniki RFID

Czytnik RFID pełni funkcję urządzenia nadawczo-odbiorczego. Jako nadajnik emituje energię pozwalającą na uaktywnienie znaczników. W niektórych systemach może również wysyłać sygnały kodów sterujących lub modyfikujących dane zapisane w pamięci znaczników. Jako odbiornik odbiera i dekoduje przesłane dane ze znacznika, które następnie może przesłać do komputera przewodowo lub bezprzewodowo. Transmisja danych pomiędzy tagiem a czytnikiem jest dwustronna. Inaczej wygląda to w przypadku zasilania, które może odbywać się tylko w jedną stronę, tj. od czytnika do znacznika.

Standardy kodowania danych w technologii RFID

Podobnie jak w przypadku innych technologii, również i w przypadku RFID można wyróżnić wiele standardów kodowania danych mających zastosowanie w systemach RFID. Wiąże się to głównie z jego techniczną realizacją, tzn. wielkością pamięci znacznika, szybkością transmisji, rodzajem kodowania itp. Do kilku najpopularniejszych standardów kodowania danych w systemach RFID należą:

- Unique – najprostszy i obecnie najpowszechniej stosowany, np. w kontrolowaniu dostępu czy rejestrowaniu czasu pracy[29];
- Hitag – ma zastosowanie w przemyśle, idealnie sprawdza się w ciężkich warunkach, gdzie wysoka niezawodność oraz bezpieczna transmisja odgrywa kluczową rolę[30];
- Mifare – opracowany przez firmę Philips, ma zastosowanie głównie do identyfikacji pracowników w postaci kard ID, w kartach bankowych (*smart-cards*) czy biletach[31];
- Icode – może być stosowany w przypadku większej odległości od czytnika do 1,5 m i powszechnie jest używany do identyfikacji i kontroli dostępu[32].

[29] Chomka M.: *Standard UNIQUE – omówienie i zastosowania* [online]. Technologie RFID I EPC [dostęp: 2019-04-23]. http://rfid-lab.pl/standard-unique-%E2%80%93-om%C3%B3wienie-i-zastosowania
[30] Netronix [dostęp: 2019-04-23]. http://netronix.pl/pl/informacje/hitag-stabilny-standard-rfid-dla-wymagajacych-aplikacji.htm
[31] PWSK [dostęp: 2019-05-27]. https://www.pwsk.pl/rfid/tagi-rfid-mifare/
[32] Netronix [dostęp: 2019-05-27]. http://netronix.pl/pl/informacje/icode-standard-rfid-dla-aplikacji-hf-1356mhz-wymagajacych-antykolizji.html

Zagrożenia bezpieczeństwa danych w systemach RFID

Oprócz wielu zalet i zastosowań RFID technologia ta ma również i wady. Ponieważ wykorzystuje spektrum elektromagnetyczne, istnieje możliwość zablokowania jej działania przez osoby dysponujące odpowiednią wiedzą, jak również podszywania się pod znacznik lub czytnik czy też podsłuchiwania transmisji. W związku z powyższym w ramach każdego ze standardów RFID wymienionych powyżej opracowano różnego rodzaju mechanizmy autentykacji, kodowania oraz szyfrowania[33]. W przypadku szyfrowania najczęściej stosowany jest algorytm AES (ang. *Advanced Encryption Standard*)[34] z kluczem 128-bitowym, którego używa się m.in. do ochrony pamięci oraz uwierzytelniania znaczników. Należy pamiętać, że w przypadku przesyłania danych wrażliwych, w tym danych osobowych, niewłaściwy sposób wykorzystania RFID może stanowić zagrożenie dla prywatności użytkowników, doprowadzając do utraty ich anonimowości. W związku z powyższym w celu zastosowania RFID trzeba dobierać odpowiedni standard, uwzględniając mechanizmy bezpieczeństwa, którymi dysponują.

3.3. Standard komunikacji bezprzewodowej krótkiego zasięgu NFC

Zasada działania NFC

Technologia NFC (ang. *Near Field Communication*) jest jednocześnie autonomicznym standardem bezprzewodowej komunikacji na bliskie odległości (do kilku centymetrów) bazującą na rozwiązaniach technologicznych RFID[35]. Działa na częstotliwości 13,56 MHz i pozwala na przesyłanie danych z szybkością od 106 kb/s do 848 kb/s. Zestaw protokołów komunikacyjnych umożliwia połączenie dwóch urządzeń elektronicznych, z których jedno jest zwykle urządzeniem przenośnym (np. smartfon), w celu nawiązania kontaktu przez ich zetknięcie lub ustawienie w odległości kilku centymetrów od siebie. Tak jak w przypadku technologii RFID również system wykorzystujący NFC wymaga dwóch zasadniczych elementów, tj. urządzenia aktywnego inicjującego połączenie oraz urządzenia docelowego. Urządzenie aktywne generuje pole RF (ang. *Radio Frequency*), które może

[33] *Bezpieczeństwo technologii RFID* [online]. Evertiq [dostęp: 2019-05-27]. http://evertiq.pl/news/16192
[34] Symetryczny szyfr blokowy przyjęty przez amerykański Narodowy Instytut Standaryzacji i Technologii (ang. NIST – *National Institute for Standards and Technology*).
[35] Near Field Communication [dostęp: 2019-05-27]. http://nearfieldcommunication.org/

zasilać pasywne urządzenie docelowe. Dzięki temu urządzenia docelowe w systemie NFC mogą przyjmować bardzo proste formy, takie jak: naklejki, breloczki, karty itp. Może on pracować w dwóch trybach:

- aktywnym – czyli takim, w którym oba urządzenia (inicjujące i docelowe) są w stanie generować sygnał. Jeśli jedno z urządzeń oczekuje na dane, to jego pole elektromagnetyczne jest wyłączone;
- pasywnym – czyli takim, w którym urządzenie inicjujące wytwarza pole elektromagnetyczne, zasilając urządzenie docelowe.

Komunikacja NFC umożliwia trzy tryby przesyłania danych[36]:

- odczytu/zapisu informacji z pasywnego znacznika NFC,
- komunikacji P2P (ang. *peer-to-peer*) pomiędzy dwoma urządzeniami aktywnymi,
- emulacji pasywnej etykiety NFC przez urządzenie aktywne.

W pierwszym wymienionym trybie odczyt/zapis informacji z pasywnego znacznika NFC odbywa się podobnie jak w przypadku technologii RFID. Również zastosowanie jest podobne. Tryb ten wykorzystuje się m.in. do celów identyfikacji użytkownika – znacznik NFC przyjmuje na ogół postać karty ID. Komunikację P2P umożliwia to, że oba urządzenia mają własne zasilanie – są to na ogół dwa urządzenia mobilne typu smartfon lub tablet. Wymiana danych działa w obu kierunkach. Po skonfigurowaniu połączenia P2P pomiędzy takimi dwoma aktywnymi urządzeniami, aby zwiększyć zasięg transmisji lub/i możliwość przesłania większej liczby danych, może zostać wykorzystana inna technologia komunikacji bezprzewodowej, jak np. Wi-Fi. Typowe zastosowanie tego trybu to wymiana danych kontaktowych (vCard) między dwoma smartfonami, przesyłanie plików, takich jak zdjęcia lub filmy, a także błyskawiczne wykonywanie przelewów. Emulacja pasywnej etykiety NFC przez urządzenie aktywne odbywa się w trybie działania pasywnym, w którym terminal mobilny (np. smartfon) zachowuje się jak inteligentny chip bezdotykowy. Ogólnie mówiąc, urządzenie aktywne emuluje (udaje) pasywny znacznik i przesyła informacje do urządzenia NFC – urządzenia inicjującego połączenie, np. do terminala płatniczego. Tryb ten może służyć do różnych celów: płatności mobilnych, weryfikacji biletów, kontroli dostępu itp.

Organizacja odpowiedzialna za promowanie technologii i ustalanie standardów NFC oraz certyfikowanie zgodności urządzeń to NFC Forum[37].

[36] UnitagNFC [dostęp: 2019-05-27]. https://www.unitag.io/nfc/what-is-nfc
[37] NFC Forum [dostęp: 2019-05-27]. https://nfc-forum.org/

Zagrożenia bezpieczeństwa danych w systemach NFC

W związku z tym że NFC wykorzystuje bezprzewodową transmisję danych, możliwe są ataki związane z tą technologią obejmujące podsłuch, uszkodzenie lub modyfikację danych czy ataki przechwytywania. Aby zapobiec występowaniu tego typu naruszeń bezpieczeństwa, stosuje się zarówno szyfrowanie transmisji danych, jak i szyfrowanie przechowywanych danych na urządzeniach NFC, m.in. istotne w przypadku kradzieży urządzenia. Bezpieczna komunikacja jest dostępna m.in. dzięki zastosowaniu algorytmów szyfrujących takich jak AES[38]. **Ze wszystkich technologii bezprzewodowych krótkiego zasięgu NFC uznaje się za najbardziej bezpieczne.** Jednym z głównych czynników, który odgrywa tutaj istotną rolę, jest zasięg działania. W przypadku zastosowań związanych np. z płatnościami urządzenia NFC muszą znajdować się w odległości do 1 cm, co bardzo utrudnia wszelkiego rodzaju podsłuchiwanie i ingerowanie w transmitowane dane.

3.4. Standard komunikacji bezprzewodowej krótkiego zasięgu Bluetooth

Zasada działania Bluetooth

Bluetooth to technologia bezprzewodowej komunikacji pomiędzy różnymi urządzeniami elektronicznymi wykorzystująca do przesyłania danych fale radiowe w paśmie ISM 2,4 GHz[39]. Nazwa technologii pochodzi od przydomka duńskiego króla Haralda Sinozębego (ang. *Harald Bluetooth*) panującego w X wieku, który zjednoczył Danię z częścią Norwegii. Technologia Bluetooth zastąpiła standard transmisji danych IrDA (ang. *Infrared Data Association*), działający w zakresie podczerwieni. Standard IrDA miał znaczne ograniczenia szczególnie z uwagi na to, że urządzenia, które komunikowały się ze sobą, „musiały się widzieć". Technologia Bluetooth powstała więc po to, aby uprościć wymianę danych i umożliwić jej prowadzenie bez ciągłego nadzoru użytkownika. Pozwala łączyć urządzenia peryferyjne z komputerem lub sprzętem mobilnym. Jest powszechnie stosowana do łączenia wszelkiego typu urządzeń komunikujących się ze smartfonem. Służy również do przesyłania plików pomiędzy urządzeniami mobilnymi. Bluetooth to otwarty standard, który opisano

[38] Heon-june K.: *A study on the Cryptographic Algorithm for NFC* [online]. Indian Journal of Science and Technology 2016, vol. *9*(37) [dostęp: 2019-05-27]. http://www.indjst.org/index.php/indjst/article/viewFile/102543/74044; Kavya S., Pavithra K., Rajaram S., Vahini M., Harini N.: *Vulnerability Analysis And Security System For NFC-Enabled Mobile Phones*. International Journal Of Scientific & Technology Research 2014, *3*(6) [dostęp: 2019-05-27]. http://www.ijstr.org/final-print/june2014/Vulnerability-Analysis-And-Security-System-For-Nfc-enabled-Mobile-Phones.pdf

[39] ISM (ang. *Industrial, Scientific, Medical*) – pasmo radiowe początkowo przeznaczone dla zastosowań przemysłowych.

w specyfikacji IEEE 802.15.1[40], rozwijany od 1994 r. Każda kolejna wersja tego standardu pozwala na coraz większą szybkość przesyłania danych, zwiększa swój zasięg działania i staje się coraz bardziej bezpieczny. Jest również kompatybilny wstecz, tzn. urządzenia z nowszą wersją są kompatybilne z wersjami starszymi. Urządzenia przesyłające dane przez Bluetooth są jednocześnie nadajnikami i odbiornikami. Mogą komunikować się jednostronnie (nadawać lub odbierać) lub dwustronnie (wykonując obie czynności naraz). Przesyłając dane, nie ustawiają się na jednej częstotliwości, ale obsługują ich aż kilkadziesiąt, synchronicznie skacząc z częstotliwości na częstotliwość. Połączone ze sobą urządzenia tworzą tzw. piconety, czyli minisieci. Do jednego urządzenia można podłączyć maksymalnie siedem innych, co zapewnia niezakłócone działanie sieci. Technologię Bluetooth można podzielić na dwie grupy: klasyczny, konwencjonalny Bluetooth – standard 1.0, 2.0, 3.0 – oraz Bluetooth o niskim poborze energii, tzw. BLE (ang. *Bluetooth Low Energy*) – standardy 4.0, 4.1, 4.2 oraz obecnie wdrażany 5.0. W przypadku drugiej grupy standardów mniej istotna stała się szybkość przesyłania danych, natomiast skupiono się na jak najmniejszym poborem energii przez urządzenia przesyłające. Obecnie to właśnie ta druga grupa standardów Bluetooth odgrywa najistotniejszą rolę w przesyłaniu danych w systemach ochrony indywidualnej na nieduże odległości – do 10 m.

Zagrożenia bezpieczeństwa danych w systemach Bluetooth

W związku z dużą popularnością tej technologii urządzenia Bluetooth są narażone na różnego rodzaju ataki, takie jak: BlueBug, Blueprinting, BlueSmack, BlueSnarf itd[41]. Dlatego też zostały opracowane różnego rodzaju mechanizmy bezpieczeństwa. Do podstawowych mechanizmów bezpieczeństwa standardu Bluetooth należy m.in. rozpoznawanie urządzeń, autoryzacja użytkowników oraz szyfrowanie przesyłanych danych. Aby zwiększyć bezpieczeństwo, można jeszcze stosować dodatkowe mechanizmy zabezpieczeń na poziomie warstwy transportowej, takie jak TLS czy IPsec[42].

Technologia Bluetooth może działać w jednym z trzech trybów bezpieczeństwa (ang. *security mode*):

1) Tryb bezpieczeństwa niechroniony, w którym nie jest wykorzystane szyfrowanie ani uwierzytelnianie.

[40] *802.15.1™. IEEE Standard for Information technology – Telecommunications and information exchange between systems – Local and metropolitan area networks – Specific requirements* [online]. New York, NY, The Institute of Electrical and Electronics Engineers, Inc. 2002 [dostęp: 2019-05-27]. http://www.diegm.uniud.it/tonello/MATERIAL/STANDARDS/802.15.1/802.15.1-2002.pdf

[41] Sapronov K.: *Bluetooth i problemy z bezpieczeństwem* [online]. Securelist [dostęp: 2019-05-27]. https://securelist.pl/ threats/5548, bluetooth_i_problemy_z_bezpieczenstwem.html

[42] Gupta S., Dham R.: *Bluetooth Low Energy 4.2 przynosi większe bezpieczeństwo komunikacji ElektronikaB2B* [online]. ElektronikaB2B [dostęp: 2019-05-27]. https://elektronikab2b.pl/prezentacja-artykul/31341-bluetooth-low-energy-42-przynosi-wieksze-bezpieczenstwo-komunikacji#.WtYchIhuaUk

2) Tryb bezpieczeństwa oparty na usłudze L2CAP, w którym jest ograniczony dostęp do urządzenia przez uwierzytelnianie po nawiązaniu połączenia.
3) Tryb bezpieczeństwa z uwierzytelnianiem na podstawie PIN-u, w którym uwierzytelnianie odbywa się przed nawiązaniem połączenia i szyfrowaniem.

Dokładne zalecenia dotyczące stosowania Bluetooth i przewodnik, w którym można znaleźć informacje dotyczące tego, jak w bezpieczny sposób korzystać z Bluetooth, znajdują się na stronie NIST (ang. *National Institute of Standards and Technology*)[43]. Do najważniejszych zaleceń należy:

- nieużywanie domyślnych ustawień urządzenia;
- ustawienie niezbędnego i wystarczającego poziomu mocy urządzeń, aby zasięg transmisji był pod kontrolą;
- włączenie uwierzytelniania na podstawie PIN-u;
- wybieranie wystarczająco długich i losowych kodów PIN zamiast statycznych i słabych, np. PIN składający się z samych zer;
- używanie jak najwyższego trybu/poziomu bezpieczeństwa;
- domyślne skonfigurowanie urządzeń Bluetooth w taki sposób, aby były niemożliwe do wykrycia i pozostawały niewykrywalne z wyjątkiem sytuacji, gdy konieczna jest wzajemna komunikacja (parowanie) pomiędzy poszczególnymi urządzeniami;
- zastosowanie szyfrowania łącza dla wszystkich połączeń.

Inne możliwe zagrożenia, wspólne dla praktycznie wszystkich technologii bezprzewodowych, to także możliwość zakłócania transmisji oraz podsłuch przesyłanych danych.

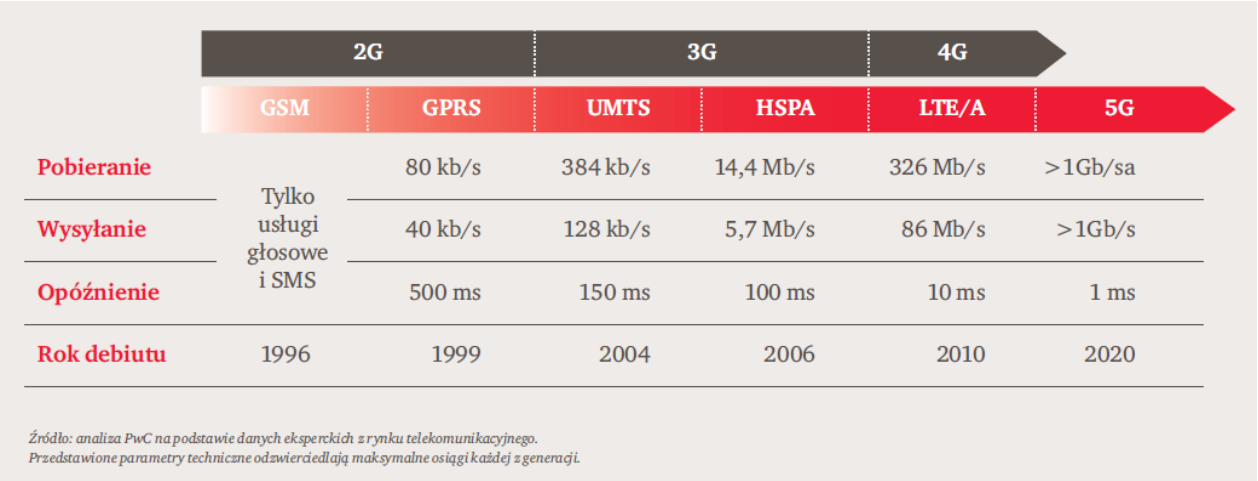
3.5. Systemy telefonii komórkowej 2G/3G/4G/5G

Zasada działania systemów telefonii komórkowej

Technologie 2G, 3G i 4G są kolejnymi generacjami systemów telefonii komórkowej[44]. Telefonię 2G nazywa się telefonią drugiej generacji. To pierwsza cyfrowa sieć telefoniczna, która zastąpiła analogową technologię 1G. Pierwszy raz została uruchomiona w Finlandii w 1991 r., a do Polski

[43] Padgette J., Scarfone K., Chen L.: *Guide to Bluetooth Security* [online]. National Institute of Standards and Technology U.S. Department of Commerce [dostęp: 2019-05-27]. https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-121r1.pdf
[44] *4G, LTE, 3G, 2G – czym różnią się od siebie poszczególne technologie?* [online]. Daily Web [dostęp: 2019-05-30]. https://dailyweb.pl/4g-lte-3g-2g-czym-roznia-sie-od-siebie-poszczegolne-technologie/

weszła jesienią 1996 r. Umożliwia wykonywanie połączeń głosowych i pakietową transmisję danych. Technologia 2G kojarzy się najczęściej z transmisją danych GPRS (ang. *General Packet Radio Service*) oraz EDGE (ang. *Enhanced Data rates for GSM Evolution*). Pierwsza z nich pozwala uzyskać transfer danych do ok. 100 kb/s, a druga do 236 kb/s (choć teoretycznie nawet do 296 kb/s)[45]. Kolejnym standardem była telefonia trzeciej generacji 3G. Pierwsza sieć 3G została uruchomiona w Japonii w 2001 r., a w Polsce dopiero w 2004 r.[46]. Wprowadziła pewnego rodzaju rewolucję, gdyż umożliwiała korzystanie z Internetu w dowolnym miejscu na świecie (oczywiście pod warunkiem że było się w zasięgu sieci 3G). To właśnie w telefonii trzeciej generacji wprowadzono możliwość przeglądania stron internetowych, przesyłania wiadomości e-mail, pobierania wideo, wideorozmów czy udostępniania zdjęć. W przypadku transmisji danych z technologią trzeciej generacji najbardziej kojarzony jest standard UMTS (ang. *Universal Mobile Telecommunications System*), zwany również Uniwersalnym Systemem Telekomunikacji Ruchomej. Standard ten umożliwia przesyłanie danych z szybkością do 384 kb/s, a dla zaimplementowanej technologii HSPA, która jest częścią standardu UMTS, transfer może sięgać nawet do 21,6 Mb/s podczas pobierania danych i 5,76 Mb/s podczas ich wysyłania przy zastosowaniu technologii MIMO. Na rysunku 7 przedstawiono rozwój technologii sieci komórkowej w Polsce od 1996 z prognozą do 2020 r.



Rys. 7. Rozwój technologii komórkowej na przykładzie Polski w okresie 1996-2020[47]

W związku z tym że sieć 3G nie spełniała do końca oczekiwań, jeżeli chodzi o jej wydajność, opracowano kolejny standard 4G. Pierwszy raz komercyjnie użyto go w Skandynawii w 2009, natomiast w Polsce w 2010 r. Aby sieć została uznana za sieć czwartej generacji, szybkość transmi-

[45] *Ewolucja telefonii komórkowej (1) – czym są sieć 1G, 2G?* [online]. Czytelnia Internetowa WBP w Opolu [dostęp: 2019-05-30]. https://internetowaopole.wordpress.com/2018/01/26/krotka-historia-telefonii-komorkowej-w-polsce/
[46] Whatsag.com [dostęp: 30 V 2019]. https://whatsag.com/
[47] Majchrzyk Ł.: *20. rocznica telefonii komórkowej w Polsce* [online]. MOBIRANK [dostęp: 2019-05-30]. https://mobirank.pl/2016/10/26/20-rocznica-telefonii-komorkowej-polsce/

sji musi znaleźć się w przedziale od 100 Mb/s do 1 Gbit/s. Tak jest właśnie w przypadku sieci 4G, która pozwala osiągać transfer danych na poziomie przynajmniej 100 Mb/s. W przypadku sieci 4G standardem bezprzewodowego transferu danych jest LTE (ang. *Long Term Evolution*), który teoretycznie pozwala osiągać szybkość transmisji rzędu 300 Mb/s w przypadku odbierania danych i ok. 80 Mb/s w przypadku ich wysyłania[48]. Obecnie trwają prace nad siecią piątej generacji. Aby sieć została uznana za standard 5G, szybkość przesyłania danych musi przekraczać 1 Gbit/s.

Zagrożenia bezpieczeństwa danych w systemach telefonii komórkowej

Podobnie jak sieci drugiej, trzeciej i czwartej generacji ewoluowały przez ostatnie lata (jak to opisano powyżej), tak również – mechanizmy bezpieczeństwa służące do ochrony transmisji danych i ruchu głosowego w tych standardach[49]. Bezpieczeństwo sieci 2G złamano już dawno, dlatego też w następnych generacjach zastosowano kolejne ulepszenia w tym zakresie. Wprowadzono standardy bezpieczeństwa 3GPP oraz nowe protokoły do silnego wzajemnego uwierzytelniania. W przypadku transmisji danych w celu zapewnienia poufności i integralności, która może być zapewniona na różnych poziomach, LTE wykorzystuje specyfikację AKA (ang. *Authentication and Key Agreement*). Do szyfrowania danych korzysta się m.in. z algorytmu AES[50]. Dodatkowo w celu ochrony poufności transmisji można stosować również tunele VPN (ang. *Virtual Private Network*). Natomiast, tak jak i w przypadku wszystkich bezprzewodowych technologii transmisji danych, sieci 2G, 3G i 4G nie są odporne na zakłócenia, np. zagłuszanie interfejsu radiowego użytkownika.

3.6. Energooszczędna, długodystansowa sieć transferu danych LoRaWAN

Zasada działania LoRaWAN

LoRaWAN (ang. *Long Range Wireless Network*) jest stosunkowo nowym standardem komunikacji bezprzewodowej przeznaczonym głównie do zastosowań IoT. Podstawowym celem wspomnianej technologii jest umożliwienie komunikacji na bardzo duże odległości przy bardzo niskim

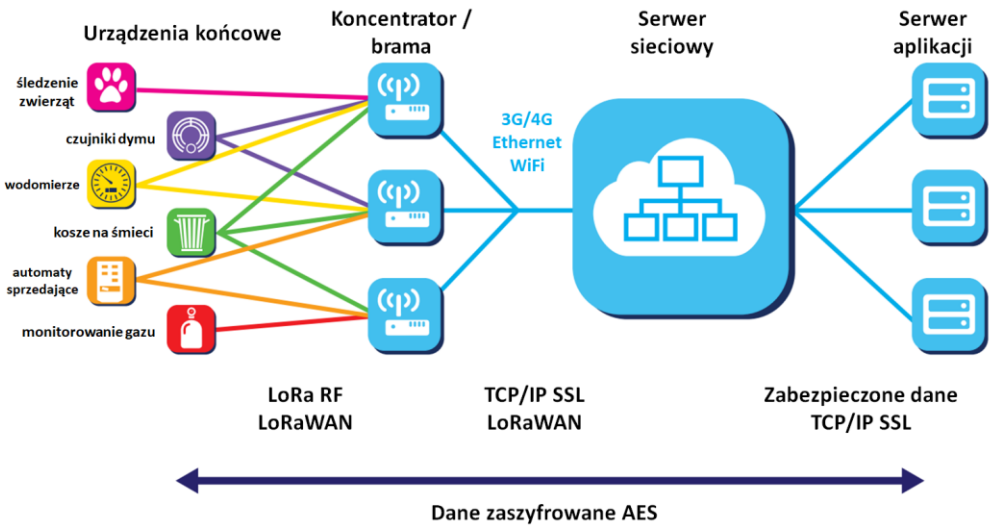
[48] Hill S.: *4G vs. LTE: The differences explained* [online]. Digital Trends [dostęp: 2019-05-30]. https://www.digitaltrends.com/mobile/4g-vs-lte/
[49] Kaczmarek S.: *Czy transmisja danych w sieciach LTE jest bezpieczna?* [online]. TELKO.IN [dostęp: 2019-05-30]. https://www.telko.in/czy-transmisja-danych-w-sieciach-lte-jest-bezpieczna,0
[50] Alt S., Fouque P.-A., Macario-rat G., Onete C., Richard B.: *A Cryptographic Analysis of UMTS/LTE AKA* [dostęp: 2019-05-29]. https://eprint.iacr.org/2016/371.pdf

zużyciu energii. Obecnie utrzymuje ją stowarzyszenie LoRa Alliance[51] składające się m.in. z firm telekomunikacyjnych.

W skład architektury LoRaWAN wchodzą cztery elementy[52]:

- urządzenia końcowe, które wysyłają i odbierają wiadomości w sieci bezprzewodowej LoRaWAN;
- bramy (ang. gateways), które odgrywają rolę przekaźników, przesyłając wiadomości z urządzeń końcowych do serwera sieciowego i na odwrót;
- serwer sieciowy, którego zadaniem jest wysyłanie i odbieranie wiadomości LoRaWAN zarówno do, jak i z urządzeń oraz komunikowanie się z serwerami aplikacji;
- serwer aplikacji, który jest miejscem docelowym przesyłanych danych.

W sieciach LoRaWAN urządzenia końcowe nie są powiązane z określoną bramą. Zamiast tego wiele bram odbiera dane przesyłane przez urządzenia końcowe. Każda brama przekazuje odebrany pakiet z urządzenia końcowego do serwera sieciowego umieszczonego na ogół w chmurze za pośrednictwem sieci komórkowej, sieci Ethernet, satelitarnej lub Wi-Fi. Następnie serwer sieciowy, który zarządza siecią i filtruje nadmiarowo odebrane pakiety, wykonuje kontrole bezpieczeństwa, planuje potwierdzenia przez optymalną bramkę i dostosowuje szybkość przesyłania danych. Architekturę sieci LoRaWAN przedstawiono na rysunku 8.



Rys. 8. Architektura sieci LoRaWAN[53]

[51] DNA of IoT [dostęp: 2019-08-21]. https://www.semtech.com/lora
[52] *LoRaWAN Overview* [online]. GitHub [dostęp: 2019-06-28]. https://github.com/Fluent-networks/floranet/wiki/LoRaWAN-Overview
[53] Na podstawie: *A technical overview of LoRa and LoRaWAN™* [online]. LoRa Alliance November 2015 [dostęp: 2019-05-29]. https://www.tuv.com/media/corporate/products_1/electronic_components_and_lasers/TUeV_Rheinland_Overview_LoRa_and_LoRaWANtmp.pdf

Tak jak wspomniano wcześniej, jedną z głównych zalet LoRaWAN jest niskie zapotrzebowanie na energię urządzeń używanych do komunikacji, co wiąże się z dostosowywaniem mocy nadajnika i szybkości transmisji do aktualnych warunków przesyłania. Kolejną istotną zaletę stanowi duży zasięg działania (do 5 km w środowisku miejskim oraz do 15 km w terenie otwartym), co umożliwia zbieranie danych z rozległego obszaru. Dzięki możliwości podłączenia do sieci LoRaWAN wielu urządzeń można ją wykorzystać w IoT do budowania inteligentnych osiedli czy nawet miast. Niestety LoRaWAN ma również pewne ograniczenia. Najważniejszym z nich jest mała szybkość transmisji danych wynosząca od 0,3 do 50 kb/s. Pomimo tego ograniczenia LoRaWAN nadaje się do przesyłania danych z czujników, w których próbkowanie odbywa się na ogół raz na sekundę, dzięki czemu idealnie nadaje się do zastosowań IoT[54].

Zagrożenia bezpieczeństwa danych w systemach LoRaWAN

Bezpieczeństwo sieci LoRaWAN odnosi się do poziomu dwóch warstw: aplikacji i sieci. Zadaniem warstwy sieci jest uwierzytelnienie poszczególnych węzłów w sieci, natomiast zadaniem warstwy aplikacji – zabezpieczenie transmisji danych, do czego wykorzystuje się algorytm AES z kluczem 128-bitowym[55].

[54] Koperski B., Nowak M., Szymborska A.: *Wykorzystanie standardu LoRaWAN do budowy bezprzewodowych siecisensorowych w inteligentnych budynkach* [online]. Napędy i Sterowanie 2016, nr 6 [dostęp: 2019-05-29]. http://yadda.icm.edu.pl/baztech/element/bwmeta1.element.baztech-5e1aeff2-041d-4972-9422-3cab08ab23f7/c/NIS-2016-6-Nowak-Wykorzystanie.pdf

[55] Aras E., Ramachandran G. S., Lawrence P., Hughes D.: *Exploring The Security Vulnerabilities of LoRa* [dostęp: 2019-05-29]. https://lirias.kuleuven.be/bitstream/123456789/587540/1/camera_ready.pdf

4. Systemy inteligentnych środków ochrony indywidualnej

W rozdziale zdefiniowano inteligentne środki ochrony indywidualnej oraz systemy inteligentnych środków ochrony indywidualnej. Przedstawiono schemat obiegu danych i informacji w systemie, w którego skład wchodzą czujniki zintegrowane ze środkami ochrony indywidualnej oraz przykłady technologii i wyrobów mających zastosowanie w systemach inteligentnych środków ochrony indywidualnej. Podsumowaniem tego rozdziału są wskazówki dotyczące dobrych praktyk w zakresie zapewnienia bezpieczeństwa obiegu danych i informacji w systemach inteligentnych środków ochrony indywidualnej.

4.1. Inteligentne środki ochrony indywidualnej i systemy inteligentnych środków ochrony indywidualnej

Określenie dowolnego wyrobu technicznego (w tym środka ochrony indywidualnej) jako inteligentnego jest różnie pojmowane w zależności od stanu techniki. Obecnie, gdy układy automatyki przemysłowej w postaci różnego rodzaju termokontrolerów powszechnie montuje się chociażby w układach ogrzewania domowego, a wyłączniki zmierzchowe są stałym elementem w wielu systemach oświetleniowych, środki ochrony indywidualnej wyposażone w podobne elementy, spełniające analogiczne funkcje, mogą już nie być uważane za inteligentne. Celowo w tym miejscu odniesiono się do zastosowania elementów automatyki przemysłowej w budownictwie. Nikt przecież obecnie nie określa domu mianem inteligentnego, jeśli wyposażono go w system ogrzewania automatycznie reagujący na zmiany temperatury zewnętrznej oraz w oświetlenie zewnętrzne z zamontowanymi czujnikami zmierzchowymi. Aby uznać dom za inteligentny, koniecznie trzeba m.in. zastosować układy automatyki przemysłowej na znacznie wyższym poziomie technicznym, który w tym przypadku odnosi się również do możliwości sterowania określonymi funkcjami za pomocą sieci komputerowej. Pozwala to na interakcję użytkownika z elementami podlegającymi sterowaniu. Jeśli do istniejących już systemów automatyki przemysłowej dodamy np. możliwość sterowania przez użytkownika za pomocą smartfona, system taki będzie najpewniej uznany za inteligentny, w przeciwieństwie do tradycyjnego systemu pozwalającego jedynie na utrzymanie zadanej temperatury dzięki wykorzystaniu typowych układów do termoregulacji. Potwierdza się tym samym przyjęte na początku tego rozdziału założenie, że **definicja inteligentnego wyrobu**

technicznego (w tym inteligentnych środków ochrony indywidualnej) będzie ewoluować wraz z rozwojem techniki.

Inteligentne środki ochrony indywidualnej są aktualnie definiowane na wiele sposobów. Przyjęta aktualnie przez CEN (fr. Comité européen de normalisation, ang. *European Committee for Standardization*) definicja inteligentnych środków ochrony indywidualnej[56] mówi, że są to środki wykonane na bazie inteligentnych materiałów tekstylnych i/lub zintegrowane z elementami elektronicznymi w celu zapewnienia dodatkowych funkcji pozwalających na interakcję użytkownika ze środowiskiem pracy. Inna – bardzo podobna definicja[57] – uściśla sposób budowania i działania tych środków, definiując je jako pojedyncze wyroby lub zestawy środków ochrony indywidualnej, wykonane z wykorzystaniem inteligentnych i/lub aktywnych materiałów lub z wbudowanymi czujnikami i układami mikro-elektro-mechanicznymi, które zapewniają realizację dodatkowych i specyficznych funkcji, w tym przede wszystkim aktywną interakcję tych środków z użytkownikiem i środowiskiem.

W obu definicjach uwagę zwraca interakcja inteligentnych środków ochrony indywidualnej z użytkownikiem. W przypadku środków ochrony indywidualnej, a właściwie inteligentnych środków ochrony indywidualnej, interakcja ta może być realizowana na wiele sposobów. Odwołajmy się do przykładu środka ochrony indywidualnej, który bez wątpienia może być określany jako inteligentny – również w kontekście drugiej z przytoczonych powyżej definicji – choć z uwagi na powszechność stosowania zwykle nie jest kojarzony z inteligentnym środkiem ochrony indywidualnej. Mowa o okularach ochronnych z zamontowanymi filtrami fotochromowymi. Powszechnie znany efekt fotochromowy pozwala na zmianę gęstości optycznej filtrów ochronnych. Jest wywołany promieniowaniem optycznym z zakresu nadfioletu (UV). Materiały fotochromowe w wyniku padania na nie promieniowania nadfioletowego ulegają zaciemnieniu, a więc zwiększa się również ich gęstość optyczna, a co za tym idzie maleje przepuszczanie promieniowania optycznego padającego na filtr. Poziom przepuszczania promieniowania widzialnego przechodzącego przez filtr fotochromowy jest więc regulowany zmianami natężenia promieniowania nadfioletowego (UV) zachodzącymi w środowisku użytkowania filtrów[58]. Zachodzi również oczywista interakcja pomiędzy okularami z filtrami fotochromowymi a użytkownikiem. Zmiana przepuszczania promieniowania widzialnego powoduje dostosowanie szerokości źrenicy użytkownika do panujących warunków

[56] *Textiles and textile products – Smart textiles – Definitions, categorisation, applications and standardization needs* [online]. NSAI Standards. Standard Recommendation S.R. CEN/TR 16298:2011 [dostęp: 2019-05-31]. https://infostore.saiglobal.com/preview/is/en/2011/srcen-tr16298-2011.pdf?sku=1505398

[57] Definicja własna.

[58] Owczarek G., Gralewicz G.: *Aktywne i pasywne optyczne filtry ochronne – zasada działania, podstawy konstrukcji*. Warszawa, CIOP-PIB 2017.

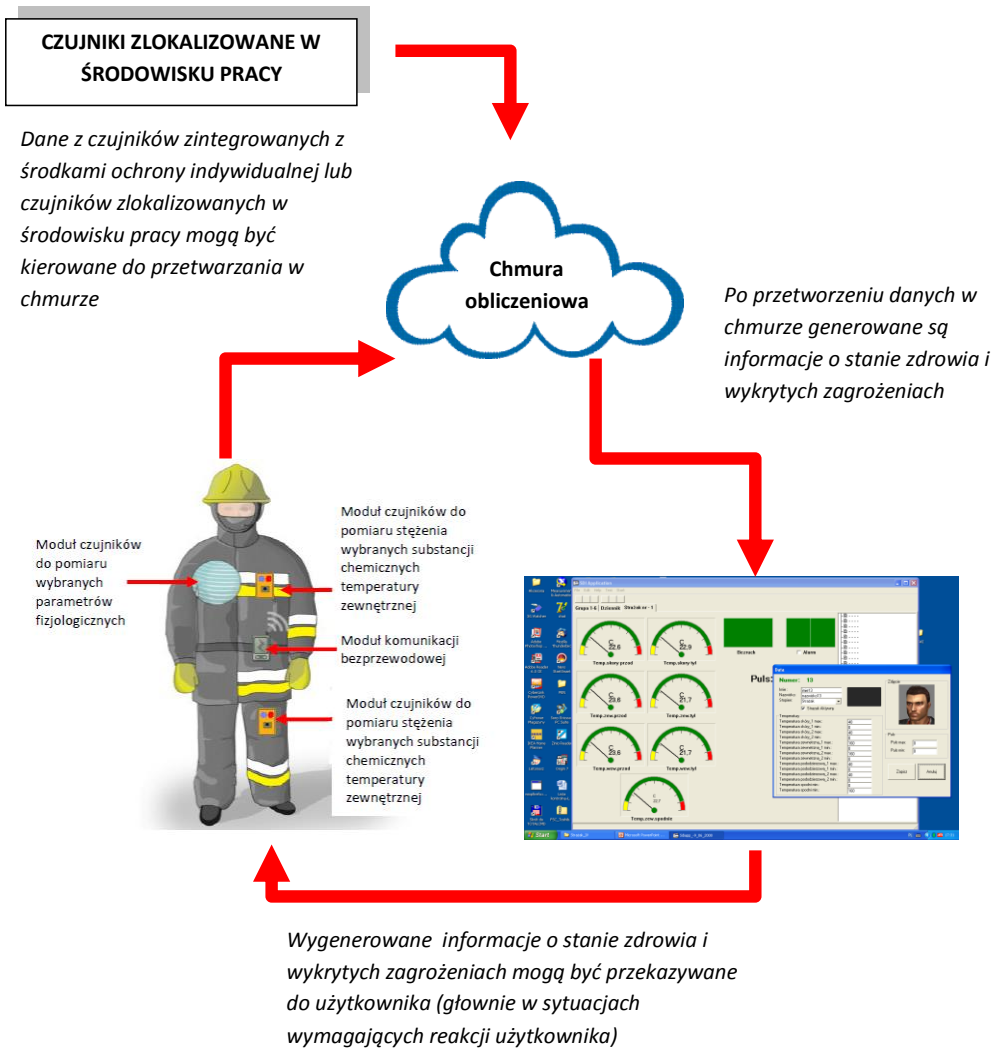
oświetlenia, zmienia się również sposób przetwarzania obserwowanych obrazów w wyniku zmiany wysycenia barwy filtrów fotochromowych. Inteligencja okularów fotochromowych, której wyrazem jest opisana interakcja z użytkownikiem, bazuje jedynie na zastosowaniu aktywnego materiału. Jego działanie inicjują warunki zewnętrzne, bez konieczności połączenia okularów fotochromowych z dodatkowym elektronicznym układem sterowania. Kolejnym przykładem środka ochrony indywidualnej, pretendującego do miana – inteligentny, jest automatyczny filtr spawalniczy. W automatycznych filtrach spawalniczych, podobnie jak dla opisanych wcześniej okularów fotochromowych, występuje zmiana gęstości optycznej. Występuje ona jednak w wyniku przyłożenia do ekranu ciekłokrystalicznego, z którego zbudowany jest filtr, napięcia powstałego na skutek zajarzenia łuku elektrycznego. W tym przypadku niezbędne jest zastosowanie elektronicznego układu sterującego. Automatyczny filtr spawalniczy może po zajarzeniu łuku elektrycznego zaciemnić się do ustalonego stałego poziomu lub zmieniać płynnie poziom przepuszczania promieniowania widzialnego generowanego podczas spawania w zależności od jego intensywności, czyli od przebiegu samego procesu spawalniczego.

Sposób, w jaki podchodzimy do definiowania inteligentnych środków ochrony indywidualnej, zależy więc nie tylko od stanu techniki, lecz również od przyjętych założeń co do rodzaju materiałów oraz od cech, które bezwzględnie muszą charakteryzować te środki. Cytowana wcześniej definicja inteligentnych środków ochrony indywidualnej przyjęta przez CEN[59] spełnia warunki co do sposobu definiowania materiałów oraz cech. W tej definicji jest mowa co prawda jedynie o inteligentnych materiałach tekstylnych, które można przecież zamienić na materiały aktywne (szersze pojęcie), ale jednak to ważna część definicji, w której jednoznacznie odniesiono się do rodzaju materiału lub zastosowanej technologii.

Mając na względzie to, że pojęcie inteligentnych środków ochrony indywidualnej na dobre zadomowiło się w piśmiennictwie z obszaru BHP, jak również ewoluowania znaczenia inteligentnych środków ochrony indywidualnej wraz z rozwojem nauki i techniki wprowadzono określenie systemów inteligentnych środków ochrony indywidualnej. Systemów, które składają się zarówno ze środków ochrony indywidualnej, czujników zintegrowanych z tymi środkami, czujników niezintegrowanych ze środkami ochrony indywidualnej oraz pozostałych elementów infrastruktury hardware'owej i oprogramowania, dzięki którym dane generowane z czujników mogą być transmitowane i przechowywane. Jeśli dzięki danym z czujników pojawią się informacje, które

[59] CEN/TR 16298:2011, Textiles and textile products. Smart textiles. Definitions, categorisation, applications and standardization needs [online]. NSAI Standards [dostęp: 31 V 2019]. https://infostore.saiglobal.com/preview/is/en/2011/srcen-tr16298-2011.pdf?sku=1505398

wywołają interakcję użytkowników, cały system będzie mógł być określany mianem systemu inteligentnego.



Rys. 9. Schemat koncepcji systemu inteligentnych środków ochrony indywidualnej[60]

Elementami przedstawionego na rysunku 9 systemu inteligentnych środków ochrony indywidualnej są: odzież ochronna z zamontowanymi modułami czujników, czujniki zlokalizowane w środowisku pracy, chmura obliczeniowa oraz komputer z oprogramowaniem obsługującym system.

Tak przedstawiona koncepcja systemów inteligentnych środków ochrony indywidualnej wpisuje się w opisaną we wstępie poradnika koncepcję IoT.

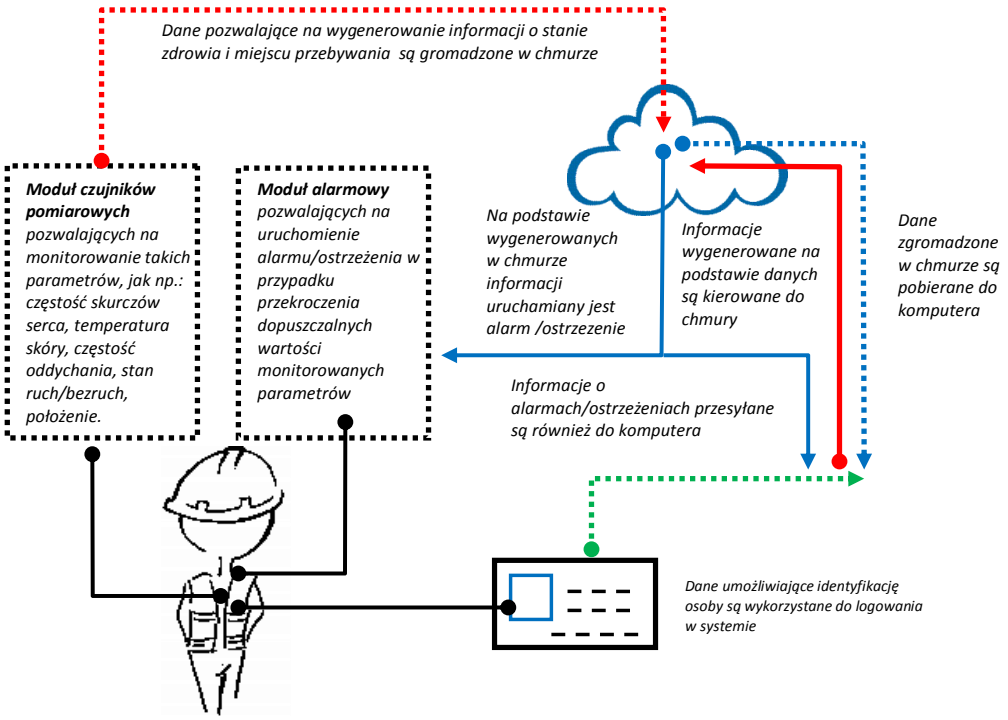
[60] W zaprezentowanej grafice wykorzystano elementy opisane w projektach: iProtect (*Intelligent PPE system for personnel in high risk and complex environments*) oraz WKP_1/1.4.4/1/2005/4/4/238/2006/U (*Ubranie strażackie nowej generacji z tekstronicznym systemem monitorowania parametrów fizjologicznych*).

W koncepcji systemów inteligentnych środków ochrony indywidualnej czujniki umożliwiające monitorowanie wybranych parametrów stanu zdrowia pracowników (użytkowników środków ochrony indywidualnej) lub parametrów środowiska pracy nie muszą być bezpośrednio zintegrowane ze środkami ochrony indywidualnej. Dane otrzymane za pośrednictwem czujników, zarówno tych zintegrowanych ze środkami ochrony indywidualnej, jak i tych ulokowanych w dowolnym miejscu środowiska pracy, mogą zostać przetransferowane do miejsca przechowywania (np. chmura) lub do innego urządzenia pozwalającego na wykorzystanie tych danych do wygenerowania użytecznych informacji, głównie w kontekście bezpieczeństwa pracy. Część informacji z powstałego zbioru może być dostępna dla użytkowników końcowych za pośrednictwem urządzeń do komunikacji zintegrowanych ze środkami ochrony indywidualnej (m.in. alarmy, interfejsy graficzne, aktuatory itp.). Otrzymane informacje mogą być również dostępne dla osób odpowiedzialnych za bezpieczeństwo i nadzór pracowników w miejscu pracy. Środki ochrony indywidualnej z zaimplementowanymi czujnikami oraz wszystkie pozostałe elementy pozwalające na transmisję, przechowywanie i analizę danych są więc określane jako system inteligentnych środków ochrony indywidualnej. W skład takiego systemu mogą wchodzić praktycznie wszystkie rodzaje stosowanych środków ochrony indywidualnej (np. odzież ochronna, przemysłowe hełmy ochronne, ochrony oczu), z którymi można zintegrować czujniki pozwalające na działanie założonych funkcji.

4.2. Obieg danych i informacji w systemach inteligentnych środków ochrony indywidualnej

W celu przeanalizowania obiegu danych i informacji w środowisku pracy opisano koncepcję przykładowego systemu (patrz rysunek 10), w którego skład wchodzą czujniki zintegrowane ze środkami ochrony indywidualnej. System ten składa się z następujących podstawowych elementów:

- identyfikatora elektronicznego w formie karty chip;
- modułu czujników pomiarowych zintegrowanych z elementami środków ochrony indywidualnej, pozwalających na monitorowanie takich parametrów, jak np.: częstość skurczów serca, temperatura skóry, częstość oddychania, stan ruch/bezruch, położenie;
- komputera z oprogramowaniem obsługującym system;
- modułu alarmowego (dla powiadomienia użytkownika o zagrożeniu zdrowia lub zabronionej lokalizacji);
- chmury obliczeniowej.



Rys. 10. Schemat przykładu obiegu danych i informacji w systemie, w którego skład wchodzą czujniki zintegrowane ze środkami ochrony indywidualnej (materiały własne autorów)

W przedstawionym przykładzie użytkownik dysponuje identyfikatorem elektronicznym (np. w formie karty chip) z zapisanymi danymi umożliwiającymi jego identyfikację. Aby zainicjować działanie systemu, konieczne jest zalogowanie się użytkownika. Musi on użyć swojego identyfikatora, na którym mogą być zapisane takie dane, jak np.: imię i nazwisko, stopień, funkcja itp. Po zalogowaniu oprogramowanie obsługujące system umożliwi skorelowanie pozostałych danych, otrzymywanych z czujników, z określoną osobą. Dane z czujników do monitorowania stanu zdrowia i położenia są przesyłane do chmury. Aby było to możliwe, zastosowane czujniki muszą być wyposażone w moduły elektroniczne umożliwiające transmisję danych w trybie online do chmury. Czujniki należy w tym przypadku rozumieć jako elementy, w skład których będą wchodzić zarówno elementy sensoryczne, jak i układy pozwalające na transmisję danych[61]. Dane zgromadzone w chmurze są następnie przesyłane do komputera z oprogramowaniem obsługującym system. Oprogramowanie to zawiera również aplikacje pozwalające na wygenerowanie informacji o stanie zdrowia i położeniu użytkownika. Wygenerowane informacje znów są kierowane do chmury, z której mogą być wysłane w formie alarmu (jeśli wystąpi zagrożenie zdrowia lub użytkownik znajdzie

[61] Owczarek G.: *Wybór czujników do monitorowania parametrów środowiska pracy i zdrowia pracowników*. W: *Nowe trendy w bezpieczeństwie pracy, środowisku i zarządzaniu*. Pod red. nauk. B. Szczuckiej-Lasoty & W. Kriesera. Katowice, Wyższa Szkoła Zarządzania Ochroną Pracy 2018, s. 295-309.

się w zabronionej lokalizacji) do użytkownika. Informacje o alarmach przesyła się za pośrednictwem chmury także do komputera, w którym jest zapisywana historia uruchamianych alarmów.

Dane mogą być również gromadzone w identyfikatorze oraz w modułach elektronicznych, które umożliwiają transmisję danych w trybie online do chmury. Zakładając, że identyfikator elektroniczny jest czymś w rodzaju dowodu osobistego, bezpieczeństwo zapisanych na nim danych leży w gestii samego użytkownika, który musi zdawać sobie sprawę, że w przypadku zagubienia lub nieuprawnionego użyczenia identyfikatora nieupoważniona osoba może zalogować się do systemu. W przypadku modułów elektronicznych umożliwiających transmisję danych do chmury zaleca się, aby moduł ten nie zapisywał danych, szczególnie danych osobowych. Oczywisty powód to ich bezpieczeństwo. Moduł elektroniczny umożliwiający transmisję danych do chmury jest zwykle zintegrowany ze środkiem ochrony indywidualnej. Może to być integracja wykonana na stałe, choć w większości przypadków moduły tego typu są dołączane do poszczególnych czujników i chowane w specjalnie zaprojektowanej do tego celu kieszeni. Jeśli więc dane otrzymane w wyniku monitorowania parametrów, będących danymi osobowymi, byłyby zapisywane i przechowywane w sposób trwały, istniałoby ryzyko dostępu do tych danych przez osoby nieuprawnione (np. obsługa magazynu, pralnie itp.).

W przedstawionym przykładzie obiegu danych i informacji w środowisku pracy widać, że aby zapewnić bezpieczeństwo generowanych w systemie danych i informacji, konieczne jest niezależne zabezpieczenie trzech warstw wchodzących w skład opisanej w rozdziale 2 architektury bezpieczeństwa IoT. Poniżej opisano kompetencje osób mających dostęp do systemu inteligentnych środków ochrony indywidualnej.

W warstwie percepcyjnej będzie to zabezpieczenie dostępu przed osobami nieuprawnionymi do wszystkich elementów fizycznych systemu opisanego na rysunku 10, czyli komputera, identyfikatora elektronicznego i czujników. **Do osób uprawnionych należy w tym przypadku zaliczyć:**

- użytkownika inteligentnych środków ochrony indywidualnej wyposażonych w czujniki,
- osobę nadzorującą pracę,
- osobę nadzorującą stan techniczny systemu,
- administratora danych.

Użytkownik, który z oczywistych względów ma dostęp do czujników i modułów alarmowych zintegrowanych ze środkiem ochrony indywidualnej, nie powinien jednak mieć możliwości ingerowania w sposób działania czujników i alarmów. Wszelkie czynności związane z obsługą, konserwacją, a także kalibracją czujników i modułów alarmowych może wykonywać jedynie osoba odpowiedzialna za stan techniczny systemu. Użytkownik ma również dostęp do identyfikatora elektro-

nicznego umożliwiającego zalogowanie się w systemie. Dostęp do tego elementu powinien być również możliwy dla osób odpowiedzialnych za stan techniczny systemu oraz nadzorujących pracę. Dostęp do komputera wraz z oprogramowaniem obsługującym system mogą mieć osoby odpowiedzialne za stan techniczny systemu i za bezpieczeństwo oraz administrator danych. Dostęp do zasobów zgromadzonych w chmurze obliczeniowej powinien mieć jedynie administrator danych.

W warstwie transportowej zabezpieczenie danych i informacji będzie polegać na szyfrowaniu ich przepływu we wszystkich opisanych w przykładzie kierunkach przepływu danych i informacji. Za szyfrowanie przepływu danych odpowiada osoba nadzorująca stan techniczny systemu.

Zabezpieczenie w warstwie aplikacji polega na szyfrowanym dostępie (login, hasło, uruchomienie aplikacji po weryfikacji linii papilarnych itp.) do wszystkich aplikacji dostępnych w chmurze i na komputerze. Za dane dotyczące zabezpieczeń w warstwie aplikacji odpowiada administrator danych, który powinien weryfikować hasła dostępu (np. w przypadku gdy są one zbyt słabe), procedury logowania oraz stan zasobów gromadzonych w pamięci komputera obsługującego system oraz w chmurze obliczeniowej.

4.3. Przykłady technologii i wyrobów do zastosowania w systemach inteligentnych środków ochrony indywidualnej

Poniżej opisano przykłady odnoszące się do dostępnych na rynku technologii i wyrobów:

- powszechnie stosowanych, których funkcjonalność odpowiada obszarowi stosowania systemów inteligentnych środków ochrony indywidualnej (opaska typu fitness);
- stosowanych poza środowiskiem pracy, lecz z uwagi na funkcjonalność oraz otwartą architekturę informatyczną mogących w przyszłości znaleźć zastosowanie również w systemach inteligentnych środków ochrony indywidualnej (system wykorzystywany w telemedycynie);
- przeznaczonych do zastosowania wyłącznie w środowisku pracy (przemysłowy hełm ochronny z czujnikami do monitorowania parametrów środowiska pracy i położenia, kurtka dla ratowników oraz system umożliwiający lokalizację pracowników).

Dla wymienionych przykładów wskazano na technologie wykorzystane do pomiaru mierzonych parametrów (czujniki). Opisano również, jak funkcjonuje obieg danych i informacji ze wskazaniem na elementy odnoszące się do bezpieczeństwa danych.

4.3.1. Monitorowanie aktywności fizycznej z wykorzystaniem inteligentnej opaski fitness[62]

Monitorowanie online aktywności fizycznej było do niedawna domeną zarezerwowaną dla wąskiej grupy odbiorców, do której zaliczali się głównie wyczynowi sportowcy. Wraz z rozwojem technologii umożliwiających wytworzenie tanich i miniaturowych czujników oraz kompletnych systemów elektronicznych pozwalających na pomiar podstawowych parametrów fizjologicznych urządzenia tego typu znalazły się w masowej produkcji, co przełożyło się na ich powszechne zastosowanie.

Z uwagi na to że jednym z najważniejszych parametrów branych pod uwagę w ocenie aktywności fizycznej jest częstość skurczów serca (HR – ang. *hart rate*)[63], urządzenia do monitorowania aktywności fizycznej składają się z pasa umieszczanego na klatce piersiowej, w którym zamontowano czujniki rejestrujące zmiany potencjału elektrycznego pozwalające na zarejestrowanie sygnałów wykorzystywanych do pomiaru częstości skurczów serca (zasada pomiaru wykorzystywana w urządzeniach EKG). Dane o częstości skurczów serca są przesyłane z pasa, zazwyczaj z wykorzystaniem technologii Bluetooth, do urządzenia umieszczanego na nadgarstku (zegarka). Na jego wyświetlaczu pojawiają się informacje o mierzonych wartościach częstości skurczów serca. Urządzenia tego typu, nazywane powszechnie pulsometrami, były na rynku jednymi z pierwszych urządzeń do monitorowania aktywności fizycznej. Stosowane są do chwili obecnej.

Opracowanie miniaturowych optycznych czujników rejestrujących przepływ krwi[64] pozwoliło na pomiar częstości skurczów serca bezpośrednio na nadgarstku – bez konieczności umieszczania czujników na klatce piersiowej. Urządzenia składające się z pasa i zegarka zostały zastąpione jednym urządzeniem, które powszechnie nazywane jest, jako inteligentna opaska fitness. Stosuje się jeszcze wiele innych określeń, takich jak: sport-testery, *smartbandy*, opaski sportowe czy opaski monitorujące aktywność fizyczną. Opaski tego typu mają głównie na celu monitorowanie aktywności fizycznej po to, by prowadzić zdrowy styl życia, stąd w nazwie pojawia się słowo „fitness". Przeznaczone są więc głównie dla osób, które chcą utrzymać dobrą formę fizyczną albo do niej powrócić. W przypadku najprostszych opasek, których nie wyposażono w czujniki podstawowych parametrów fizjologicznych, a jedynie w czujniki ruchu (akcelerometry), ich funkcjonalność sprowadza się do liczenia kroków. Na podstawie tych danych obliczany jest przebyty dystans oraz oszacowuje

[62] W opisie przykładu posłużono się najczęściej używaną w powszechnym obiegu nazwą opasek do monitorowania wybranych parametrów fizjologicznych i aktywności fizycznej.
[63] Potocznie używane jest również określenie puls, odnoszące się do tętna, czyli falistego ruchu naczyń tętniczych. Ruch ten zależy zarówno od częstości skurczów serca, jak i od elastyczności ścian samych naczyń tętniczych.
[64] Zasada działania czujników optycznych opiera się na pomiarze wartości strumienia światła rozproszonego od przepływającej krwi. Wartość tego strumienia zależy od dynamiki przepływu wymuszonej częstością skurczów serca.

się liczbę spalonych kalorii. Droższe, bardziej zaawansowane technologicznie opaski mają wbudowane optyczne czujniki częstości skurczów serca, temperatury oraz moduł lokalizacji GPS (ang. *Global Positioning System*). Mogą również komunikować się z urządzeniami mobilnymi, takimi jak smartfony lub laptopy.

Czujniki zamontowane w opasce pozwalają na pomiar następujących danych:

- liczba kroków (czujnik ruchu),
- aktualna lokalizacja (GPS),
- częstość skurczów serca (optyczny czujnik przepływu krwi).

Na podstawie tych danych można otrzymać informacje o:

- przebytym dystansie i wysokości, na której przebywa użytkownik (na podstawie danych z GPS);
- aktywności fizycznej (na podstawie danych o częstości skurczów serca);
- liczbie spalonych kalorii (algorytm do oszacowania ilości spalonych kalorii wykorzystuje dane o liczbie wykonanych kroków, przebytym dystansie, z uwzględnieniem charakterystyki przebytej drogi, oraz częstości skurczów serca).

Dodatkowo, wykorzystując połączenie Bluetooth 4.0 i synchronizację ze smartfonem, opaska może odbierać powiadomienia z portali społecznościowych, SMS-y, sprawdzać nieodebrane połączenia telefoniczne oraz sterować zestawem słuchawkowym.

Ze zbioru informacji, które można otrzymać dzięki opasce fitness, w środowisku pracy mogą być przydatne głównie informacje o przebytym dystansie i wysokości, na której przebywa użytkownik, oraz aktywności fizycznej. **Informacje te mogą być wykorzystane w celu monitorowania bezpieczeństwa pracownika.** Wykorzystując opaski typu fitness, należy mieć jednak na względzie, że pochodzące z niej informacje mogą być wysyłane do osobistego smartfona użytkownika (np. do aplikacji Endomondo), a w dalszej kolejności do chmury (m.in. portali społecznościowych typu Facebook lub innych serwisów). W tym miejscu można postawić pytanie, czy użytkownik świadomie chce się podzielić swoimi wrażliwymi danymi (np. stan aktywności fizycznej lub miejsce aktualnego przebywania), czy też aplikacja robi to bez jego wiedzy? Taki obieg danych i informacji sprawia, że w przypadku stosowania przez pracowników w miejscu pracy opasek typu fitness pracodawca, a więc podmiot odpowiedzialny za bezpieczeństwo pracownika, nie ma praktycznie żadnej możliwości kontroli nad danymi i informacjami o pracowniku. **Z tego względu stosowanie powszechnie dostępnych opasek typu fitness w celu monitorowania parametrów fizjologicznych lub aktywności fizycznej pracowników w miejscu pracy jest mocno dyskusyjne. Pomimo funkcjonalności tego typu opasek, które mogą być bardzo przydatne w procesie monitorowania**

bezpieczeństwa pracowników, istnieje uzasadnione ryzyko związane z brakiem możliwości zapewnienia przez pracodawcę bezpiecznego obiegu danych i informacji.

Nie należy jednak wykluczać możliwości stosowania opasek typu fitness w miejscu pracy. Aby jednak było to bezpieczne, pod kątem bezpieczeństwa danych, konieczne jest opracowanie szczegółowej procedury obiegu danych i stworzenie dla konkretnego zastosowania architektury bezpieczeństwa, w której uwzględnione zostaną niezbędne zabezpieczenia we wszystkich z trzech omawianych w rozdziale 2 elementach architektury bezpieczeństwa IoT (warstwa percepcyjna, transportowa i aplikacji).

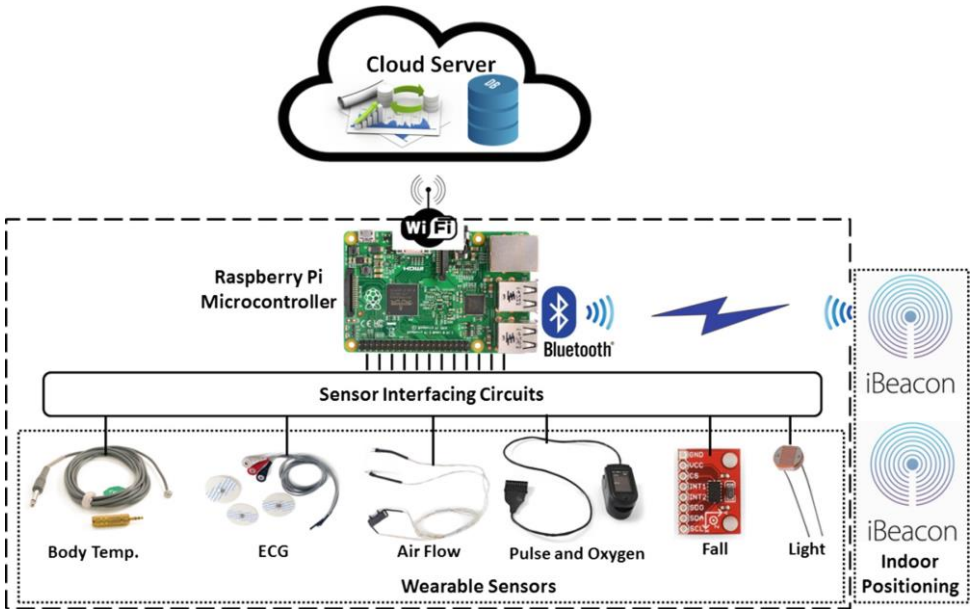
Jeśli jednak opaski tego typu miałyby mieć zastosowanie w środowisku pracy z uwagi na możliwość monitorowania parametrów istotnych dla zdrowia pracowników, należy w tym przypadku unikać wycieku danych, co dla powszechnie stosowanych urządzeń działających w odwołaniu do koncepcji IoT (również dla opasek typu fitness) ma zasadnicze znaczenie.

Poniżej sformułowano najważniejsze wskazówki do realizacji dobrych praktyk w zakresie ochrony danych monitorowanych z wykorzystaniem opasek typu fitness:

1. Aby zapobiec przypadkowemu wyciekowi danych, nie zaleca się wysyłania danych monitorowanych do serwerów pracodawcy lub rozwiązań chmurowych.
2. Najlepiej aby dane były rejestrowane lokalnie na urządzeniu stosowanym przez pracownika.
3. Tylko w sytuacjach zagrażających życiu, jak np. zaburzenia akcji serca, znaczne wahania temperatury, bezruch użytkownika itp., urządzenie powinno wysłać istotne dane, m.in. z informacją o zagrożeniu życia i zdrowia pracownika lub stanie ruch/bezruch.
4. Dane powinny być wysyłane najlepiej w postaci kodu, którego interpretację będą znać służby ratownicze pracodawcy przewidziane do działania w tego typu sytuacjach. Wraz z danymi o stanie zdrowia powinny być przesyłane dane o lokalizacji pracownika.
5. Wszystkie dane powinny być wysyłane w formie niejawnej, czyli zaszyfrowanej.
6. W przypadku potrzeby analizy przez służby ratownicze historii danych otrzymanych w wyniku monitoringu pracownika (np. analiza częstości skurczów serca lub temperatury w czasie, analiza położenia itp.) dane zgromadzone w urządzeniu stosowanym przez pracownika mogą być wykorzystane.
7. Po skończeniu pracy przez użytkownika jego dane wrażliwe powinny zostać usunięte z urządzenia automatycznie.
8. Niewskazane jest wysyłanie przez pracownika swoich danych wrażliwych do portali społecznościowych.

4.3.2. Biometryka – monitorowanie stanu zdrowia i aktywności fizycznej

Zaprezentowany poniżej system monitorowania stanu zdrowia i wspomagania aktywności fizycznej (ang. *Health Monitoring System for Active and Assisted Living*) jest typowym przykładem rozwiązania działającego na podstawie koncepcji IoT. Został on skonstruowany i opisany przez School of Engineering and Technology (USA) oraz Electronics and Electrical Communications (Egipt)[65]. **Dzięki otwartej strukturze systemu informatycznego rozwiązania z zakresu transmisji danych mogą być w stosunkowo prosty sposób zaadaptowane do systemów inteligentnych środków ochrony indywidualnej. Adaptacja oznacza w tym przypadku również możliwość zapewnienia przez pracodawcę kontroli nad bezpieczeństwem obiegu danych i informacji.** Czujniki zastosowane w tym systemie pozwalają nie tylko na monitorowanie aktywności fizycznej, lecz również na zbieranie informacji pod kątem medycznej oceny stanu zdrowia. Schemat działania prezentowanego systemu przedstawiono na rysunku 11.



Wyjaśnienie oznaczeń na rysunku:
Cloud Server – serwer w chmurze; Raspberry Pi Microcontroler – Mikrokontroler; Bluetooth – standard bezprzewodowej komunikacji krótkiego zasięgu; Sensor Interfacing Circuits – zastosowane czujniki; Body Temp. – czujnik temperatury; ECG – czujnik częstotliwości i rytmów skurczów serca; Air Flow – czujnik częstotliwości oddechu; Pulse and Oxygen – czujniki częstotliwości oddechu i tlenu rozpuszczonego w krwi; Fall – czujniki upadku/położenia; Light – czujnik natężenia światła; iBeacon – urządzenie do identyfikacji; Indoor Positioning – pozycjonowanie

Rys. 11. Schemat działania *Health Monitoring System for Active and Assisted Living*[66]

[65] Abdelgawad A., Yelamarthi K., Khattab A.: *IoT – Based Health Monitoring System for Active and Assisted Living* [dostęp: 2019-06-14]. http://www.springer.com/cda/content/document/cda_downloaddocument/9783319619484-c2.pdf?SGWID=0-0-45-1611806-p180938434

[66] Abdelgawad A., Yelamarthi K., Khattab A.: *IoT – Based Health Monitoring System for Active and Assisted Living* [dostęp: 2019-06-14]. http://www.springer.com/cda/content/document/cda_downloaddocument/9783319619484-c2.pdf?SGWID=0-0-45-1611806-p180938434

System przeznaczony jest do monitorowania podstawowych funkcji fizjologicznych, szczególnie w obszarze tzw. telemedycyny. Zbierane są następujące dane o stanie fizjologicznym użytkownika systemu:

- ilość tlenu rozpuszczonego we krwi,
- częstość i rytm skurczów serca (EKG),
- częstość oddechów,
- temperatura ciała.

Dodatkowo system rejestruje również położenie (dane z akcelerometru) oraz natężenie światła w otoczeniu użytkownika. Dane z czujników (EKG, częstość oddechów, temperatura, natężenie światła i położenie) przesyłane są przewodowo na odpowiednie wejścia do mikrokontrolera *Raspberry Pi*. Lokalizowanie użytkownika odbywa się na podstawie sygnałów odbieranych z wykorzystaniem iBeacon, które transmituje się zgodnie z protokołem BLE (ang. *Bluetooth Low Energy*). Następnie transmituje się dane do chmury przez Internet za pośrednictwem technologii Wi-Fi. W celu bezpiecznej, szyfrowanej transmisji danych wykorzystany jest protokół TLS (ang. *Transport Layer Security*) oraz algorytm kryptograficzny AES (ang. *Advanced Encryption Standard*).

Zalety prezentowanego rozwiązania wynikają głównie z możliwości wykrywania nieprawidłowości związanych z zaburzeniami rytmu serca oraz oddychania. Zastosowanie czujnika pozwalającego na detekcję położenia umożliwia powiadamianie osób nadzorujących działanie systemu o upadku monitorowanej osoby. Czujnik natężenia światła pełni funkcję, którą można porównać z automatycznym sterowaniem przesłoną w aparacie fotograficznym. Tak jak przesłona aparatu fotograficznego może automatycznie dostosować swoją wielkość do natężenia oświetlenia zewnętrznego, aby uzyskać optymalny efekt oświetlenia matrycy aparatu, tak w przypadku omawianego systemu czujnik natężenia światła pozwala na zwiększanie lub zmniejszanie intensywności sztucznego oświetlenia w korelacji ze zmieniającymi się warunkami zewnętrznymi.

Na temat wad prezentowanego systemu do monitorowania stanu zdrowia i wspomagania aktywności fizycznej mogliby się wypowiedzieć jego użytkownicy. Niezależnie od wad mogących wynikać np. z określonych rozwiązań w zakresie ergonomii i komfortu użytkowania (np. dopasowanie czujników, wygoda użytkowania itp.) do wad należy bezsprzecznie zaliczyć podatność na zakłócenia transmisji danych przesyłanych drogą bezprzewodową oraz możliwość wycieku lub utraty danych. W przypadku opisanego rozwiązania Health Monitoring System for Active and Assisted Living danymi, które mogą być traktowane jako wrażliwe, są dane o wszystkich rejestrowanych przez system parametrach fizjologicznych użytkownika.

Sposób, w który należy zabezpieczyć dane generowane w systemie (opisanym w powyższym przykładzie), jest analogiczny do dobrych praktyk opisanych w poprzednim podrozdziale (podrozdział 4.3.1).

4.3.3. Monitorowanie środowiska pracy z wykorzystaniem przemysłowego hełmu ochronnego

Konstrukcja przemysłowych hełmów ochronnych umożliwia dołączenie do skorupy hełmu dodatkowych elementów. Przemysłowe hełmy ochronne integrowane są z innymi rodzajami środków ochrony indywidualnej (głównie osłony twarzy i ochronniki słuchu) oraz takimi elementami, jak np.: latarki, systemy do komunikacji głosowej lub moduły systemów rzeczywistości wzbogaconej.

Inteligentny kask przeznaczony jest głównie do stosowania w sektorze budownictwa, zarówno na przestrzeniach zamkniętych, jak i otwartych. Na skorupie hełmu zamontowano czujniki temperatury oraz system nawigacji satelitarnej GPS. Czujniki te pozwalają na monitorowanie miejsca przebywania pracowników użytkujących hełm oraz temperatury w ich bezpośrednim otoczeniu.

Do transmisji danych zbieranych z czujnika temperatury i systemu GPS w przypadku użytkowania hełmu w pomieszczeniach zamkniętych wykorzystywany jest Bluetooth o niskim poborze energii, tzw. BLE. Dane transmitowane są do smartfona, a następnie z wykorzystaniem protokołu transmisji danych MQTT (ang. *MQ Telemetry Transport*) przenoszone do bazy danych w chmurze. W przypadku użytkowania hełmu na zewnątrz do transmisji danych wykorzystuje się standard LoRa. Dane o temperaturze i położeniu transmituje się w pierwszej kolejności do routera, a następnie z wykorzystaniem protokołu sterowania transmisją TCP (ang. *Transmission Control Protocol*) do serwera LoRa. Z serwera LoRa dane z wykorzystaniem MQTT trafiają do chmury. W celu bezpiecznej, szyfrowanej transmisji danych używa się protokołu SSL (ang. *Secure Socket Layer*) lub TLS (*Transport Layer Security*). W zastosowanych protokołach do szyfrowania danych wykorzystano algorytm kryptograficzny – symetryczny szyfr blokowy AES (ang. *Advanced Encryption Standard*).

System GPS umożliwia określenie miejsca przebywania pracownika oraz wysokości, na której się on znajduje. W przypadku placu budowy informacja o położeniu i wysokości pracownika pełni kluczową funkcję z uwagi na występowanie takich zagrożeń, jak: ruchome elementy infrastruktury, magazyny składowania niebezpiecznych substancji, głębokie wykopy i wiele innych. W zależności od miejsca przebywania pracownika na placu budowy konieczne jest zastosowanie odpowiednich środków ochrony indywidualnej. Ponieważ przemysłowe hełmy ochronne są priorytetowym elementem zabezpieczenia pracownika na każdym placu budowy, zamontowane na hełmie czujniki monitorujące wybrane parametry środowiska pracy mogą być również źródłem informacji

o konieczności zastosowania innych, niezbędnych do danego miejsca środków ochrony indywidualnej. Zastosowanie czujnika temperatury pozwala z kolei na kontrolę temperatury w bezpośrednim otoczeniu pracownika, co przekłada się na ocenę zagrożeń wywołanych promieniowaniem termicznym, które może być konsekwencją zarówno ekstremalnych warunków pogodowych (w sposób szczególny upały i intensywne nasłonecznienie), jak i nieprzewidzianych katastrof (np. pożary).

Zastosowanie energooszczędnej, długodystansowej sieci transferu danych (LoRa) pozwala na transmisję danych na duże odległości. W warunkach zabudowy miejskiej zasięg sieci LoRa szacowany jest na 5 km, a w terenie otwartym aż do ok. 15 km, co wystarcza, by mógł być zastosowany na placach budowy.

Wady, które można przypisać prezentowanemu rozwiązaniu, odnoszą się głównie do podatności na zakłócenia transmisji danych przesyłanych drogą bezprzewodową. Wszystkie rozwiązania, w których zastosowano systemy łączności bezprzewodowej, mogą być zakłócane przez wysokoenergetyczne pole elektromagnetyczne. Na placach budowy może być ono wytwarzane m.in. przez urządzenia spawalnicze. Niezależnie od zastosowanych technologii do zabezpieczania transmisji danych – również w systemach dedykowanych do konkretnych zastosowań – zawsze istnieje ryzyko wycieku lub utraty przesyłanych i gromadzonych danych. W przypadku opisanego rozwiązania – inteligentnego hełmu – danymi, które mogą być traktowane jako dane wrażliwe, są wyłącznie dane o miejscu przebywania pracownika.

4.3.4. Monitorowanie częstości skurczów serca, temperatury otoczenia i lokalizacji z wykorzystaniem odzieży ochronnej

Firma NOKIA znana jest głównie z produkcji telefonów komórkowych i smartfonów. W kooperacji z południowokoreańską marką modową Kolon Industries oraz czeskim producentem oprogramowania GINA Software Ltd. NOKIA opracowała kurtkę CHASE LifeTech FR (CHASE jest akronimem od Connected Health and Safety Equipment). Wyposażono ją w moduły z czujnikami do pomiaru częstości skurczów serca, temperatury otoczenia, położenia (GPS) oraz ruchu (akcelerometr).

Moduły pozwalające na zamontowanie czujników rozmieszczono wokół rękawów i na klatce piersiowej. Zaletą konstrukcji modułowej jest to, że czujniki można umieścić w położeniu odpowiednim do potrzeb (np. czujniki temperatury mogą być umieszczone na rękawach i/lub na klatce piersiowej). Dane generowane z czujników umieszczonych na kurtce są przesyłane bezprzewodowo w czasie rzeczywistym do bazy, gdzie przeprowadza się ich analizę pod kątem bezpieczeństwa

użytkownika kurtki. Sprawdza się częstość skurczów serca, temperaturę wokół użytkownika oraz jego bieżące położenie.

Zastosowanie modułowej konstrukcji ma jeszcze jedną bardzo ważną zaletę. Do modułów zaimplementowanych na powierzchni kurtki można będzie w przyszłości montować czujnik dowolnego innego parametru pozwalającego na monitorowanie środowiska pracy (np. czujniki przekroczenia stężenia niebezpiecznych gazów i par[67]). Warunkiem jest oczywiście taka konstrukcja czujnika, aby jego sygnał wyjściowy był kompatybilny z elektronicznym układem pomiarowym zamontowanym w kurtce.

Producent – w dostępnych materiałach na temat wyrobu – nie podaje szczegółów odnoszących się do sposobu transmisji danych. Można się jedynie domyślać, że wykorzystywany jest do tego celu standard telefonii komórkowej. W tym przypadku pracodawca powinien zwrócić szczególną uwagę na to, aby dane i informacje zgromadzone z wykorzystaniem czujników zintegrowanych z kurtką nie przedostały się do przestrzeni publicznej, więc również w tym przykładzie mają zastosowanie wskazówki co do dobrych praktyk w zakresie ochrony danych monitorowanych z wykorzystaniem opasek typu fitness (podrozdział 4.3.1).

4.3.5. Monitorowanie czasu pracy i lokalizacji pracownika

Informacja o aktualnym miejscu przebywania pracownika jest coraz częściej pożądana w miejscu pracy nie tylko z uwagi na nadzór i kontrolę, lecz przede wszystkim z uwagi na bezpieczeństwo. Służą do tego systemy umożliwiające śledzenie osób (ang. *personal tracking systems*). Należy jednak pamiętać, że dane określające lokalizację konkretnej osoby mogą być traktowane jako dane wrażliwe. **Głównym zadaniem systemu śledzenia osób jest określenie dokładnej lokalizacji danej osoby, mierzonej w regularnych odstępach czasu.** Zapisane dane dotyczące lokalizacji mogą być przechowywane w jednostce śledzącej lub mogą być przesyłane do bazy danych lokalizacji centralnej systemu. Zastosowania systemów do śledzenia osób są bardzo różnorodne. Jednym z głównych zastosowań jest śledzenie położenia osób z różnego rodzaju dolegliwościami zdrowotnymi oraz osób przebywających w miejscach, w których występują poważne zagrożenia dla zdrowia i życia, np. alpinistów, strażaków przeprowadzających akcję w płonącym budynku[68] itp. Zarówno w przypadku śledzenia osób z dolegliwościami zdrowotnymi, jak i śledzenia osób przebywających w niebezpiecznych miejscach dokładna lokalizacja ułatwia dotarcie do śledzonego człowieka w celu

[67] Sawyer J.: *Nokia's latest high-tech jacket is perfectly, accidentally on-trend* [online]. HIGHSNOBIETY [dostęp: 2019-06-14]. https://www.highsnobiety.com/p/nokia-rescue-jacket/
[68] Fischer C., Gellersen H.: *Location and navigation support for emergency responders: a survey* [online]. LOCATION-BASED SERVICES [dostęp: 2019-06-14]. https://core.ac.uk/download/pdf/1549878.pdf

udzielenia mu niezbędnej pomocy lub umożliwia uruchomienie innych systemów ostrzegających o powstających zagrożeniach.

Jedną z podstawowych klasyfikacji systemów do śledzenia osób jest podział ze względu na miejsce zastosowania:

- systemy stosowane wewnątrz budynków,
- systemy stosowane na zewnątrz budynków.

W obu wymienionych przypadkach wykorzystywane są inne technologie stosowane do transmisji danych. W przypadku śledzenia osób w budynkach używa się technologii Wi-Fi, RFID lub Bluetooth, natomiast w przypadku terenów otwartych – głównie GPS. Systemy śledzenia stosowane wewnątrz budynków określa się również jako IPS (ang. *Indoor Positioning System*)[69].

Do śledzenia osób za pomocą systemu PEOPLE wykorzystuje się cztery podstawowe elementy:

- opaskę na nadgarstek,
- przepustkę,
- urządzenie typu BLE Gateway (ang. *Bluetooth Smart Gateway*),
- urządzenie monitorujące.

Opaska na nadgarstek i przepustka to urządzenia elektroniczne wysyłające sygnały, które są odbierane przez urządzenie typu BLE Gateway. Do transmisji tych sygnałów wykorzystywana jest technologia Bluetooth Smart. Przesyłanie danych z BLE Gateway do systemu monitorującego odbywa się z wykorzystaniem technologii Wi-Fi lub GSM.

Zastosowane w systemie PEOPLE technologie bezprzewodowe do transmisji danych są bardzo wygodne z punktu widzenia samego użytkowania. Stosując te technologie, należy pamiętać jednak o prawidłowym zabezpieczeniu transmisji danych i wybierać najmocniejsze, dostępne na chwilę obecną protokoły do zabezpieczania danych. W przypadku technologii Wi-Fi to protokół WPA2, który pozwala szyfrować transmisję danych najmocniejszym na chwilę obecną symetrycznym algorytmem kryptograficznym AES (ang. *Advanced Encryption Standard*). Jedną z wad rozwiązań bezprzewodowych jest możliwość zakłócania sygnału. Standardy Bluetooth i Wi-Fi pracują na często-

[69] Olevall A. H., Fuchs M.: *Indoor Navigation and Personal Tracking System Using Bluetooth Low Energy Beacons* [dostęp: 2019-06-14]. https://uu.diva-portal.org/smash/get/diva2:1148761/FULLTEXT01.pdf

tliwości 2,4 GHz, a więc na częstotliwości, na której pracuje większość popularnych urządzeń powszechnego użytku, takich jak np. telefony, mikrofalówki lub alarmy samochodowe. Działanie tych urządzeń może zakłócać sygnały przesyłane w systemie PEOPLE. Opisany powyżej system jest jednym z wielu tego typu rozwiązań dostępnych na rynku. Inne przykłady podobnych rozwiązań, opartych na systemie lokalizacji ludzi w budynkach, to np. system Indor Tracking[70] lub IndoorAtlas[71].

4.4. Dobre praktyki zapewniania bezpieczeństwa obiegu danych i informacji w systemach inteligentnych środków ochrony indywidualnej

Analiza opisanego powyżej schematu obiegu danych i informacji w systemach inteligentnych środków ochrony indywidualnej oraz przykładów technologii i wyrobów do zastosowania w systemach inteligentnych środków ochrony indywidualnej pozwala na sformułowanie podstawowego wykazu dobrych praktyk. Dobrych praktyk, których realizacja podnosi poziom bezpieczeństwa obiegu danych i informacji generowanych, przechowywanych i transmitowanych w systemach inteligentnych środków ochrony indywidualnej.

Dbałość o bezpieczeństwo danych i informacji należy zarówno do pracodawcy, jak i do użytkowników środków ochrony indywidualnej. Z uwagi na to, że pracodawca jest zobowiązany wyposażyć pracowników w niezbędne na danym stanowisku pracy środki ochrony indywidualnej, to na nim spoczywa największa odpowiedzialność również w zakresie zapewnienia bezpieczeństwa danych i informacji generowanych, przechowywanych i transmitowanych w systemach inteligentnych środków ochrony indywidualnej. Pracodawca, wyposażając pracowników w systemy inteligentnych środków ochrony indywidualnej, musi mieć świadomość, że dane, które będą otrzymywane z wykorzystaniem tych systemów, mogą mieć charakter wrażliwy, a więc mogą być danymi osobowymi w rozumieniu Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (Dziennik Urzędowy UE L 119/1 z 4 maja 2016)[72].

[70] Indoor Tracking [online]. Infsoft [dostęp: 2019-06-17]. https://www.infsoft.com/solutions/indoor-tracking
[71] IndoorAtlas [dostęp: 2019-06-17]. http://www.indooratlas.com/
[72] W rozdziale 5 przedstawiono analizę Rozporządzenia o ochronie danych osobowych w kontekście ochrony danych, które są generowane, przechowywane i transmitowane w systemach inteligentnych środków ochrony indywidualnej.

Jeśli do zbioru danych należeć będą m.in. dane ujawniające informacje o stanie zdrowia (np. dane otrzymywane podczas monitorowania częstości skurczów serca, temperaturze lub innych parametrów fizjologicznych), pracownik musi wyrazić zgodę na ich[73]. Uzyskanie takiej zgody od pracownika musi być poprzedzone poinformowaniem go o tym, które dane będą rejestrowane, w jaki sposób i w jakim zakresie będą przetwarzane oraz o gwarancjach odnoszących się do bezpieczeństwa ich przetwarzania.

Najważniejszym elementem gwarancji bezpieczeństwa przetwarzania danych jest opracowanie i wdrożenie architektury bezpieczeństwa dla użytkowanego systemu inteligentnych środków ochrony indywidualnej. Architektura bezpieczeństwa, zgodnie z tym co zostało opisane w rozdziale 2, powinna składać się z warstwy percepcyjnej, transportowej i aplikacji. Zabezpieczenie w warstwie percepcyjnej polega na uniemożliwieniu osobom nieuprawnionym dostępu do urządzeń gromadzących, przechowujących i transmitujących dane, w warstwie transportowej – na szyfrowaniu przepływu danych i informacji, a w warstwie aplikacji – na szyfrowanym dostępie (login, hasło, uruchomienie aplikacji po weryfikacji linii papilarnych itp.) do wszystkich aplikacji zastosowanych w systemach inteligentnych środków ochrony indywidualnej.

Wszystkim danym należy zapewnić integralność, poufność i dostępność. Integralność oznacza, że dane są kompletne i zebrane z wystarczającą dokładnością, aby wygenerować informacje, które chcemy otrzymać. Należy również zapewnić odpowiednie metody przetwarzania tych danych. Poufność oznacza, że zbierane dane/informacje są dostępne jedynie dla osób do tego upoważnionych. Dostępność to zapewnienie osobom upoważnionym dostępu do danych/informacji zawsze, gdy jest taka potrzeba.

Dla zapewnienia bezpieczeństwa danych generowanych, przechowywanych i transmitowanych w systemach inteligentnych środków ochrony indywidualnej, funkcjonujących w ramach wdrożonej architektury bezpieczeństwa, niezmiernie istotne jest, aby pracodawca spełnił następujące warunki:

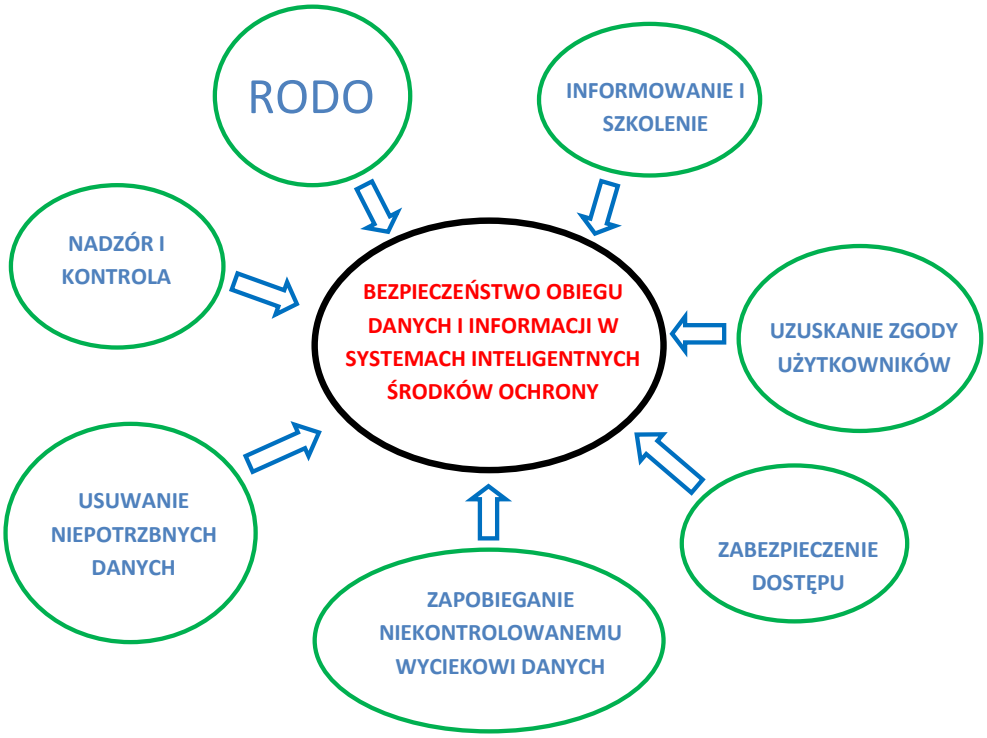
1. **Zapewnienie wymogów prawnych.** Procedury generowania, przechowywania i transmisji danych powinny być zgodne z obowiązującymi przepisami (RODO). Pracodawca powinien powołać administratora, czyli osobę odpowiedzialną za bezpieczeństwo danych osobowych. Powinny zostać wyznaczone osoby odpowiedzialne za nadzór nad pracą osób wyposażonych w inteligentne środki ochrony indywidualnej oraz za nadzór nad stanem technicznym całego systemu inteligentnych środków ochrony indywidualnej.

[73] Wzory oświadczenia pracowników na zgodę na przetwarzanie danych osobowych pozyskiwanych w miejscu pracy zamieszczono w podrozdziale 5.4.

2. **Informowanie i szkolenie pracowników.** Pracownicy użytkujący systemy inteligentnych środków ochrony indywidualnej powinni zostać poinformowani o procedurze generowania, przechowywania i transmitowania danych, a także przeszkoleni w zakresie obsługi użytkowanych systemów inteligentnych środków ochrony indywidualnej oraz procedur związanych z dostępnością danych.
3. **Uzyskanie zgody pracowników.** Pracownicy użytkujący systemy inteligentnych środków ochrony indywidualnej muszą wyrazić zgodę na przetwarzanie ich danych osobowych[74].
4. **Zabezpieczenie dostępu.** Dostęp do elementów systemu inteligentnych środków ochrony indywidualnej mogą mieć wyłącznie osoby upoważnione[75].
5. **Zapobieganie niekontrolowanemu wyciekowi danych.** Aby zapobiec przypadkowemu wyciekowi danych, nie zaleca się wysyłania do serwerów pracodawcy lub rozwiązań chmurowych danych monitorowanych. Najlepiej aby dane były rejestrowane lokalnie na urządzeniu stosowanym przez pracownika. Powinno się przesyłać dane tylko w uzasadnionych przypadkach. Pod żadnym pozorem nie należy umieszczać danych (w szczególności danych wrażliwych) na portalach społecznościowych.
6. **Usuwanie niepotrzebnych danych.** Po skończeniu pracy wszystkie niepotrzebne dane, które zostały zgromadzone podczas użytkowania systemów inteligentnych środków ochrony indywidualnej, należy usunąć. Zalecane jest, aby usuwanie niepotrzebnych danych odbywało się automatycznie.
7. **Kontrola i nadzór nad systemem.** Sprawne działanie systemu inteligentnych środków ochrony indywidualnej, zarówno w aspekcie technicznym (m.in. testypenetracyjne, kontrola czujników itp.), jak i pod kątem przestrzegania procedur związanych m.in. z weryfikacją haseł oraz osób upoważnionych do dostępu do poszczególnych elementów systemu. To ważny element bezpieczeństwa danych i informacji.

Na rysunku 12 przedstawiono schematycznie siedem wymienionych powyżej elementów, których realizacja podnosi poziom bezpieczeństwa obiegu danych i informacji generowanych, przechowywanych i transmitowanych w systemach inteligentnych środków ochrony indywidualnej.

[74] Wzory oświadczenia pracowników na zgodę na przetwarzanie danych osobowych pozyskiwanych w miejscu pracy zamieszczono w podrozdziale 5.4.
[75] Przykład podziału kompetencji, jakie powinny posiadać osoby mające dostęp do systemu inteligentnych środków ochrony indywidualnej, opisano w podrozdziale 4.2.



Rys. 12. Schematyczne przedstawienie elementów, których realizacja podnosi poziom bezpieczeństwa obiegu danych i informacji generowanych, przechowywanych i transmitowanych w systemach inteligentnych środków ochrony indywidualnej (materiały własne autorów)

W stosowaniu wymienionych powyżej dobrych praktyk bardzo pomocna jest znajomość szczegółowych zaleceń w zakresie ochrony danych i zapewnienia cyberbezpieczeństwa (zaleceń obowiązujących dla wszystkich obszarów, a więc również dla systemów inteligentnych środków ochrony indywidualnej) oraz właściwa interpretacja aktualnie obowiązujących przepisów z dziedziny ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych. Zagadnienia te opisano w rozdziale 5 i 6.

5. Ochrona danych w świetle obowiązujących przepisów

W rozdziale przedstawiono analizę Rozporządzenia o ochronie danych osobowych w kontekście ochrony danych, które są generowane, przechowywane i transmitowane w systemach inteligentnych środków ochrony indywidualnej.

5.1. Definicja danych osobowych

Ochrona danych dotyczy w sposób szczególny danych określanych jako dane osobowe. Pojęcie danych osobowych ma swoje znaczenie prawne. Zgodnie z obowiązującą do maja 2018 r. w Polsce ustawą o ochronie danych osobowych[76] **dane osobowe to wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej**. Każdemu obywatelowi Polski przysługuje prawo do ochrony danych osobowych. W ramach reformy systemu ochrony danych osobowych w UE przyjęto Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (Dziennik Urzędowy UE L 119/1 z 4 maja 2016).

Z wielu przesłanek za wprowadzeniem nowych regulacji prawnych w zakresie ochrony danych osobowych na pierwszym miejscu był bardzo dynamiczny rozwój technologii informatycznych. Na globalnym rynku pojawiły się firmy mające w swoich zasobach ogromne ilości danych, wśród których są również dane osobowe o charakterze wrażliwym, i operujące nimi. Firmy te, jak np. Google, Facebook lub Apple, nie podlegały bezpośrednio obowiązującej do niedawna dyrektywie 95/46/WE[77]. Świadomość zagrożenia, które może stwarzać niczym niekontrolowany sposób przetwarzania danych osobowych, sprawiła, że korporacje zarządzające i przetwarzające dane osobowe inicjowały własne działania w zakresie ochrony danych osobowych. Generowało to jednak koszty i nie zapewniało wymaganej spójności w zakresie ochrony danych o charakterze wrażliwym. Inną ważną przesłanką za opracowaniem nowego Rozporządzenia o ochronie danych osobowych – obowiązującego we wszystkich krajach UE – są różnice w sposobie wdrażania dyrektywy

[76] Ustawa z dn. 29 sierpnia 1997 r. o ochronie danych osobowych (DzU 1997, nr 133, poz. 883). Ustawa przestała obowiązywać 25 maja 2108 r.
[77] Dyrektywa 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych.

95/46/WE przez poszczególne kraje członkowskie UE[78]. Nowe Rozporządzenie obowiązuje bez żadnych zmian we wszystkich krajach UE. **W Polsce zaczęło obowiązywać od 25 maja 2018 r.**

Zgodnie z nowym Rozporządzeniem **dane osobowe oznaczają informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą")**. Możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak: imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej[79].

5.2. Analiza Rozporządzenia Parlamentu Europejskiego i Rady (UE) z dnia 27 kwietnia 2017 r. pod kątem ochrony danych osobowych, które są generowane, przechowywane i transmitowane w systemach inteligentnych środków ochrony indywidualnej

Analiza Rozporządzenia umożliwia udzielenie odpowiedzi na kilka zasadniczych pytań, które mają wskazać na to, czy procedury przetwarzania danych osobowych generowanych, przechowywanych i transmitowanych w systemach inteligentnych środków ochrony indywidualnej podlegają zawartym w nim przepisom. A jeśli tak, to w jaki sposób należy zorganizować procedurę przetwarzania tych danych, aby była ona zgodna z obowiązującym prawem. Pytania te są następujące:

1. Czy przetwarzanie danych osobowych, które są generowane, przechowywane i transmitowane w systemach inteligentnych środków ochrony indywidualnej, mieści się w zakresie Rozporządzenia?
2. Czy procedurę przetwarzania danych osobowych, które są generowane, przechowywane i transmitowane w systemach inteligentnych środków ochrony indywidualnej, można uznać za legalną w myśl Rozporządzenia? Jeśli tak, to jakie warunki należy spełnić, aby zapewnić legalność przetwarzania tych danych?
3. Jak należy interpretować ogólne zasady przetwarzania danych – określone w Rozporządzeniu – w odniesieniu do procedur przetwarzania danych osobowych, które są genero-

[78] Gawrońska-Pyciak A.: *Nowe regulacje wprowadzone Rozporządzeniem o ochronie danych osobowych*. Materiały szkoleniowe. Warszawa, Studium Prawa Europejskiego 2017.
[79] Art. 4, Definicje, 1).

wane, przechowywane i transmitowane w systemach inteligentnych środków ochrony indywidualnej?

4. Czy dane przetwarzane w systemach inteligentnych środków ochrony indywidualnej wymagają zgody osób, których dotyczą, oraz czy należą one do szczególnej kategorii danych osobowych?
5. Jakie prawa przysługują osobom, których dotyczą generowane, przechowywane i transmitowane w systemach inteligentnych środków ochrony indywidualnej dane osobowe?
6. Czy do przetwarzania danych osobowych, które są generowane, przechowywane i transmitowane w systemach inteligentnych środków ochrony indywidualnej, konieczne jest określenie obowiązków osób odpowiedzialnych za przetwarzanie danych? Jeśli tak, to jaki jest podstawowy zakres tych obowiązków?

Analizując treść Rozporządzenia, można udzielić następujących odpowiedzi na postawione powyżej pytania. W przeprowadzonej analizie odwołano się do konkretnych (zacytowanych w odsyłaczach) artykułów Rozporządzenia.

Ad 1

Rozporządzenie ma zastosowanie do przetwarzania danych osobowych stanowiących część zbioru danych lub mających stanowić część zbioru danych w każdy sposób, w tym całkowicie lub częściowo zautomatyzowany[80]. Zakres ten określa więc każdy sposób przetwarzania danych osobowych. **Tak mocne określenie zakresu danych osobowych, których przetwarzanie podlega przepisom nowego Rozporządzenia, nie budzi żadnych wątpliwości, że również dane generowane, przechowywane i transmitowane w systemach inteligentnych środków ochrony indywidualnej będą podlegać przepisom Rozporządzenia.** Analiza określonych w nim wyjątków w sytuacjach szczególnych[81] nie obejmuje również przypadku, w którym dane osobowe generowane, przechowywane i transmitowane w systemach inteligentnych środków ochrony indywidualnej mogłyby zostać wyłączone spod uregulowań obowiązujących w Rozporządzeniu.

Ad 2

Jeśli przeprowadzona powyżej analiza (patrz Ad. 1) potwierdziła, że dane osobowe generowane, przechowywane i transmitowane w systemach inteligentnych środków ochrony indywidualnej

[80] Art. 2, Materialny zakres stosowania.
[81] Art. 49, Wyjątki w szczególnych sytuacjach.

podlegają uregulowaniom zapisanym w nowym Rozporządzeniu, to pytanie o legalność procedury ich przetwarzania może wydawać się bezzasadne. Zasady regulujące sposób przetwarzania danych osobowych zdefiniowane w nowym Rozporządzeniu[82] określają jednak warunki, które muszą być spełnione, aby ich przetwarzanie było zgodne z prawem. Jest ono legalne, jeśli zostanie spełniony co najmniej jeden z poniższych warunków:

„a) osoba, której dane dotyczą, wyraziła zgodę na przetwarzanie swoich danych osobowych w jednym lub większej ilości celów,

b) przetwarzanie jest niezbędne do wykonywania umowy, której stroną jest osoba, której dane dotyczą, lub do podjęcia działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy,

c) przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze,

d) przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej,

e) przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi,

f) przetwarzanie jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora lub przez stronę trzecią z wyjątkiem sytuacji, w których nadrzędny charakter wobec tych interesów mają interesy lub podstawowe prawa i wolności osoby, której dane dotyczą, wymagające ochrony danych osobowych, w szczególności gdy osoba, której dane dotyczą, jest dzieckiem[83]”.

Z przedstawionego powyżej zestawienia przypadków, z których co najmniej jeden musi być spełniony, decydujących o legalności przetwarzania danych osobowych, jednoznacznie wynika, że **w przypadku danych osobowych generowanych, przechowywanych i transmitowanych w systemach inteligentnych środków ochrony indywidualnej warunkiem legalności przetwarzania tych danych jest zgoda osoby, której dotyczą**.

[82] Art. 5, Zasady dotyczące przetwarzania danych.
[83] Art. 6, Zgodność przetwarzania z prawem.

Ad 3

Warunki zacytowane w powyższym punkcie (patrz Ad. 2) odnoszą się do tzw. **zasady legalności, rzetelności i przejrzystości** w procesie przetwarzania danych osobowych. Przekładają się one także na kolejne ogólne zasady przetwarzania danych osobowych, które mówią, że powinno ono być:

- ograniczone co do celu, czyli powinno się ograniczać wyłącznie do konkretnych uzasadnionych potrzeb oraz niezbędnych elementów (**zasada ograniczenia celu i minimalizacji danych**);
- prawidłowe (**zasada prawidłowości**), co oznacza, że jeśli w procesie przetwarzania danych pojawią się dane nieadekwatne do celów, w których są one przetwarzane, powinno się je natychmiast usunąć, a wszelkie nieprawidłowości niezwłocznie sprostować;
- ograniczone, procedura przechowywania danych nie może trwać dłużej, niż jest to niezbędne (**zasada ograniczenia przechowywania**). Jednocześnie forma przechowywania danych musi uniemożliwić identyfikację osoby, której dane dotyczą (tzw. dane pseudonimizowane[84], czyli dane, których nie można przypisać konkretnemu podmiotowi bez użycia dodatkowych informacji);
- integralne i poufne (**zasada integralności i poufności**), co oznacza, że dane powinny być przetwarzane w sposób zapewniający bezpieczeństwo, w tym całkowitą ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz ich przypadkową utratą. Poufność i integralność należy zapewnić, stosując odpowiednie środki techniczne i organizacyjne;
- rozliczalne (**zasada „rozliczalności"**), czyli nadzorowane przez administratora, który jest odpowiedzialny za przestrzeganie wszystkich przepisów obowiązujących w zakresie ochrony danych osobowych.

Ad 4

Odpowiadając na pytanie 2 (patrz Ad. 2), wykazano bezspornie, że **dane przetwarzane w systemach inteligentnych środków ochrony indywidualnej wymagają zgody osób, których te dane dotyczą**. Analizując definicje, opracowane na użytek nowego Rozporządzenia[85], należy zauważyć, że w większości przypadków dane z systemów inteligentnych środków ochrony indywidualnej, które będą klasyfikowane jak dane osobowe, to dane dotyczące zdrowia oraz dane biometryczne. **Dane dotyczące zdrowia oznaczają dane osobowe o zdrowiu fizycznym lub psychicznym osoby**

[84] Art. 4, Definicje, 5).
[85] Art. 4, Definicje.

fizycznej – w tym o korzystaniu z usług opieki zdrowotnej – ujawniające informacje o stanie jej zdrowia[86]. **Dane biometryczne oznaczają z kolei dane osobowe, które wynikają ze specjalnego przetwarzania technicznego i dotyczą cech fizycznych, fizjologicznych lub behawioralnych osoby fizycznej** oraz umożliwiają lub potwierdzają jednoznaczną identyfikację tej osoby (wizerunek twarzy lub dane daktyloskopijne)[87].

Dane te nie należą jednak do kategorii szczególnych danych osobowych. W ujęciu nowego Rozporządzenia pojęcie szczególności danych osobowych odnosi się do sytuacji, w których dane osobowe mogą być przetwarzane. Artykuł 49 Rozporządzenia określa również wyjątki w szczególnych sytuacjach: „W razie braku decyzji stwierdzającej odpowiedni stopień ochrony określonej w art. 45 ust. 3 lub braku odpowiednich zabezpieczeń określonych w art. 46, w tym wiążących reguł korporacyjnych, jednorazowe lub wielokrotne przekazanie danych osobowych do państwa trzeciego lub organizacji międzynarodowej mogą nastąpić wyłącznie pod warunkiem, że: a) osoba, której dane dotyczą, poinformowana o ewentualnym ryzyku, z którymi – ze względu na brak decyzji stwierdzającej odpowiedni stopień ochrony oraz na brak odpowiednich zabezpieczeń – może się dla niej wiązać proponowane przekazanie, wyraźnie wyraziła na nie zgodę”.

Analizując powyższy zapis w kontekście danych osobowych generowanych, przechowywanych i transmitowanych w systemach inteligentnych środków ochrony indywidualnej, należy wnioskować, że nawet w przypadku jeśli osoba, której dane dotyczą, zostanie poinformowana o ryzyku związanym z brakiem odpowiedniego stopnia ochrony, to dane nie mogą być przetwarzane. Zapis art. 49 mówi jedynie o „jednorazowym lub wielokrotnym przekazaniu danych osobowych do państwa trzeciego lub organizacji międzynarodowej”.

Ad 5

Prawa przysługujące osobom, których dotyczą dane generowane, przechowywane i transmitowane w systemach inteligentnych środków ochrony indywidualnej, wynikają bezpośrednio z interpretacji ogólnych zasad przetwarzania danych (patrz Ad. 3). W sposób szczególny ma tutaj zastosowanie zasada przejrzystości. Przewiduje ona m.in., że **osoba, której dane dotyczą, musi być poinformowana o prowadzeniu operacji przetwarzania i jej celach**. Ponadto należy poinformować osobę, której dane dotyczą, o profilowaniu[88] oraz jego konsekwencjach. Osoba, której dane dotyczą, jest uprawniona, aby uzyskać od administratora potwierdzenie tego faktu. Szczegółowy

[86] Art. 4, Definicje, 15).
[87] Art. 4, Definicje, 14).
[88] Art. 4, Definicje, 4).

wykaz uprawnień znajduje się w art. 15 nowego Rozporządzenia[89]. Osoba, której dane dotyczą, ma również prawo do następujących informacji:

- cel przetwarzania danych;
- kategorie danych;
- odbiorcy lub kategorie odbiorców, którym dane osobowe zostaną ujawnione;
- planowany czas przechowywania danych;
- prawo zażądania od administratora sprostowania, usunięcia lub ograniczenia przetwarzania danych lub do wniesienia sprzeciwu wobec przetwarzania;
- o prawie wniesienia skargi do organu nadzorczego;
- o źródle pozyskania danych osobowych, jeśli nie zostały one zebrane bezpośrednio od danej osoby;
- o procedurach związanych ze zautomatyzowaniem przetwarzania danych (w przypadku systemów inteligentnych środków ochrony indywidualnej mogą to być np. informacje o działaniu algorytmów decyzyjnych działających na podstawie danych z czujników itp.).

Osoba, której dane dotyczą, ma również prawo do otrzymania kopii przetwarzanych danych.

Ad 6

Rozporządzenie definiuje jednoznacznie osobę administratora oraz podmiotu przetwarzającego. Administrator to osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych. Jeżeli są one określone w prawie UE lub w prawie państwa członkowskiego, to również w prawie UE lub w prawie państwa członkowskiego może zostać wyznaczony administrator lub mogą zostać podane konkretne kryteria jego wyznaczania[90]. Pojęcie podmiotu przetwarzającego oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który przetwarza dane osobowe w imieniu administratora[91].

Administrator oraz podmiot przetwarzający są zobowiązani do wdrożenia odpowiednich środków technicznych odpowiadających danemu ryzyku, uwzględniając następujące elementy:

- pseudonimizację i szyfrowanie danych osobowych;
- zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania;

[89] Art. 15, Prawo dostępu przysługujące osobie, której dane dotyczą.
[90] Art. 4, Definicje, 7).
[91] Art. 4, Definicje, 8).

- zdolność do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego i technicznego;
- regularne testowanie, mierzenie i ocenianie skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania.

Nie obowiązuje już Ustawa o ochronie danych osobowych z dn. 29 sierpnia 1997 r., w myśl której każdy administrator danych był zobowiązany do prowadzenia dokumentacji ochrony danych osobowych. **Nowe Rozporządzenie wprowadza obowiązek tzw. rejestrowania czynności przetwarzania**[92]**.** Rejestry te muszą mieć formę pisemną oraz elektroniczną. Zamieszcza się w nich m.in. następujące informacje:

- imię i nazwisko lub nazwę, dane kontaktowe administratora oraz wszelkich współadministratorów, a także – gdy ma to zastosowanie – przedstawiciela administratora oraz inspektora ochrony danych;
- cele przetwarzania;
- opis kategorii osób, których dane dotyczą, oraz kategorii danych osobowych;
- kategorie odbiorców, którym dane osobowe zostały lub zostaną ujawnione, w tym odbiorców w państwach trzecich lub w organizacjach międzynarodowych;
- jeżeli jest to możliwe, planowane terminy usunięcia poszczególnych kategorii danych;
- jeżeli jest to możliwe, ogólny opis technicznych i organizacyjnych środków bezpieczeństwa.

Na podstawie przeprowadzonej analizy zapisów nowego Rozporządzenia należy więc stwierdzić, że:

- Procedura przetwarzania danych osobowych, które są generowane, przechowywane i transmitowane w systemach inteligentnych środków ochrony indywidualnej, podlega Rozporządzeniu Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r.
- Dane te mogą być legalnie przetwarzane, z uwzględnieniem wszystkich ogólnych zasad przetwarzania danych osobowych określonych w Rozporządzeniu[93] (rzetelność i przejrzystość, ograniczenie celu, minimalizacja danych, prawidłowość, bezpieczeństwo oraz integralność i poufność, a także „rozliczalność"). W sposób szczególny należy się skoncentrować m.in. na zasadzie ograniczonego przechowywania. Zasada ta mówi jasno, że w przypadku danych pozyskiwanych do celów statystycznych lub archiwalnych (np. z uwagi na konieczność prowadzenia statystyk o wybranych parametrach fizjologicznych pracowników w zależności od warunków pracy) dane mogą być przechowywane przez dłuższy czas,

[92] Art. 30, Rejestrowanie czynności przetwarzania.
[93] Art. 5, Zasady dotyczące przetwarzania danych.

niż to niezbędne. Należy więc zdefiniować, co się kryje pod pojęciem dłuższy czas, jak również wprowadzić wszelkie możliwe i dostępne środki techniczne w celu zabezpieczenia archiwalnych zbiorów danych.

- Na przetwarzanie danych osobowych, które są generowane, przechowywane i transmitowane w systemach inteligentnych środków ochrony indywidualnej, wymagana jest zgoda osób, których dane te dotyczą[94]. Zarządza nimi administrator. Do jego zadań należy również dokumentowanie wszelkich naruszeń oraz w przypadku, gdy do nich dochodzi, wdrażanie stosownych działań zaradczych[95]. Osoba, której dane dotyczą, może zażądać od administratora niezwłocznego usunięcia jej danych osobowych, a administrator ma obowiązek bez zbędnej zwłoki je usunąć (szczegółowy zakres okoliczności, w których obowiązuje ta zasada, opisano w Rozporządzeniu).

5.3. Wdrażanie przepisów Rozporządzenia Parlamentu Europejskiego i Rady (UE) z dnia 27 kwietnia 2017 r. w kontekście danych osobowych, które są generowane, przechowywane i transmitowane w systemach inteligentnych środków ochrony indywidualnej

Przeprowadzona powyżej analiza nowego Rozporządzenia została ograniczona do tych zapisów, które należy bezwzględnie uwzględnić w procedurze przetwarzania danych oraz które mogą być generowane, przechowywane i transmitowane w środkach ochrony indywidualnej. Przepisy zawarte w Rozporządzeniu wymusiły reformę krajowego porządku prawnego. Rozporządzenie jest stosowane we wszystkich krajach UE, co naturalnie prowadzi do ujednolicenia prawa materialnego. Niezbędne stało się więc wprowadzenie nowych uregulowań proceduralnych określających m.in. status i kompetencje organów ds. ochrony danych osobowych w każdym państwie UE. W związku z powyższym polski ustawodawca będzie musiał dokonać przeglądu wielu aktów prawnych m.in. po to, aby ujednolicić stosowane do chwili obecnej definicje oraz wprowadzić nowe[96]. Poniżej (patrz tabela 1) zestawiono najważniejsze definicje z nieobowiązującej już ustawy o ochronie danych osobowych oraz nowego Rozporządzenia. Mają one odniesienie do danych, które mogą

[94] Art. 7, Warunki wyrażenia zgody.
[95] Art. 33, Zgłaszanie naruszeń ochrony danych osobowych organowi nadzorczemu.
[96] Na podstawie: *Nowe ramy ochrony danych osobowych w UE. Wyzwania dla Polski. Raport pokonferencyjny* [dostęp: 2017-09-23]. https://www.cyberlaw.pl/wp-content/uploads/2015/09/RPK_Reforma_ochrony_danych_osobowych_24.09.15.pdf

być generowane, przechowywane i transmitowane w systemach inteligentnych środków ochrony indywidualnej.

Tabela 1. Zestawienie najważniejszych definicji z ustawy o ochronie danych osobowych i nowego Rozporządzenia z przykładami. Mają one odniesienie do danych, które mogą być generowane, przechowywane i transmitowane w systemach inteligentnych środków ochrony indywidualnej (SIŚOI)

Zapis w ustawie o ochronie danych osobowych (Art. 7)	Zapisy w Rozporządzeniu	Odniesienie do SIŚOI
Zbiór danych – każdy mający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego czy jest on rozproszony lub podzielony funkcjonalnie.	**Zbiór danych** oznacza uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego czy jest on scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie.	W SIŚOI mogą to być: – imię i nazwisko, – data urodzenia / wiek, – dane o monitorowanych parametrach fizjologicznych, – dane o schorzeniach (np. dane mogące mieć wpływ na prawidłowy dobór środków ochrony indywidualnej, takie jak ostrość wzroku itp.).
Przetwarzanie danych – jakiekolwiek operacje wykonywane na danych osobowych, takie jak: zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych.	**Przetwarzanie** oznacza operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, takie jak: zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie przez przesyłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie.	Przetwarzanie danych z sensorów/czujników służących do monitorowania parametrów fizjologicznych oraz danych o schorzeniach, a także do identyfikacji pracownika (imię i nazwisko, wiek itp.).
System informatyczny – zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych.	Brak definicji. W tekście Rozporządzenia pojawia się określenie **system informacyjny**.	Sensory/czujniki zintegrowane ze środkami ochrony indywidualnej oraz sensory i czujniki zlokalizowane w środowisku pracy oraz poza nim, moduły przetwarzania danych, oprogramowanie do generowania/monitorowania, przechowywania i transmitowania danych w SIŚOI.

Tabela 1. cd.

Zapis w ustawie o ochronie danych osobowych (Art. 7)	Zapisy w Rozporządzeniu	Odniesienie do SIŚOI
Zabezpieczenie danych w systemie informatycznym – wdrożenie i eksploatacja stosownych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem.	Procedura **bezpieczeństwa danych osobowych** została opisana w sekcji 2 (*Bezpieczeństwo danych osobowych*).	Oprogramowanie oraz procedury techniczne i organizacyjne zapewniające bezpieczeństwo danych generowanych/ monitorowanych, przechowywanych i transmitowanych w SIŚOI.
Usuwanie danych – zniszczenie danych osobowych lub taka ich modyfikacja, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą.	Procedura **usuwania danych** została opisana w sekcji 3 (*Sprostowanie i usuwanie danych*).	Oprogramowanie oraz procedury techniczne i organizacyjne zapewniające trwałe usunięcie danych generowanych/ monitorowanych, przechowywanych i transmitowanych w SIŚOI.
Administrator danych – organ, jednostka organizacyjna, podmiot lub osoba, o których mowa w art. 3 (patrz DzU 1997, nr 133, poz. 883), decydujące o celach i środkach przetwarzania danych osobowych.	**Administrator** oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych. Jeżeli cele i sposoby takiego przetwarzania są określone w prawie UE lub państwa członkowskiego, to również w prawie UE lub państwa członkowskiego może zostać wyznaczony administrator lub mogą zostać określone konkretne kryteria jego wyznaczania.	Osoba odpowiedzialna w firmie za eksploatację SIŚOI (np. upoważniony pracownik służby BHP).
Zgoda osoby, której dane dotyczą – oświadczenie woli, którego treścią jest zgoda na przetwarzanie danych osobowych tego, kto składa oświadczenie; zgoda nie może być domniemana lub dorozumiana z oświadczenia woli o innej treści, może być odwołana w każdym czasie.	**Zgoda osoby, której dane dotyczą,** oznacza dobrowolne, konkretne, świadome i jednoznaczne okazanie woli, w formie oświadczenia lub wyraźnego działania potwierdzającego. Osoba, której dane dotyczą, przyzwala na przetwarzanie jej danych osobowych.	Oświadczenie osoby użytkującej SIŚOI i wyrażającej zgodę na przetwarzanie danych osobowych.

Tabela 1. cd.

Zapis w ustawie o ochronie danych osobowych (Art. 7)	Zapisy w Rozporządzeniu	Odniesienie do SIŚOI
Odbiorca danych – każdy komu udostępnia się dane osobowe, z wyłączeniem: a) osoby, której dane dotyczą; b) osoby upoważnionej do przetwarzania danych; c) przedstawiciela, o którym mowa w art. 31a (patrz DzU 1997, nr 133, poz. 883); d) podmiotu, o którym mowa w art. 31 (patrz DzU 1997, nr 133, poz. 883); e) organów państwowych lub organów samorządu terytorialnego, którym dane są udostępniane w związku z prowadzonym postępowaniem.	**Odbiorca** oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, któremu ujawnia się dane osobowe niezależnie od tego, czy jest stroną trzecią.	Upoważniona osoba nadzorująca wykonywanie pracy i odpowiedzialna za bezpieczeństwo pracy.

5.4. Oświadczenie pracownika o wyrażeniu zgody na przetwarzanie danych osobowych pozyskiwanych w miejscu pracy

W celu spełnienia wymogów prawnych Rozporządzenia pracownicy, których dane osobowe będą generowane, przechowywane i transmitowane, muszą wyrazić na to zgodę. Wzór proponowanego oświadczenia przedstawiono w tabeli 2.

Tabela 2. Wzór proponowanego oświadczenia pracownika, w którym wyraża on zgodę na przetwarzanie danych osobowych

1. **<Imię i nazwisko>** …….. wyrażam zgodę na przetwarzanie następujących danych osobowych: <*należy wyszczególnić wszystkie rodzaje i formy danych osobowych, które będą przetwarzane, np.:* **imię i nazwisko, wiek, tętno, temperatura skóry**>
2. **Zostałem poinformowany przez pracodawcę o:** – rodzaju i formie przetwarzanych danych osobowych, – sposobie i zakresie przetwarzania tych danych, – gwarancjach odnoszących się do ochrony przetwarzanych danych.
3. **Data i podpis pracownika** ……..
4. **Informacje dla pracownika** **W związku z zastosowaniem na** <*podać stanowisko pracy, np.* **stanowisku piecowego**> **systemu** <*podać funkcje systemu, np.* **do monitorowania tętna i temperatury skóry**> **będą zbierane dane osobowe pracownika** <*należy wyszczególnić wszystkie rodzaje i formy danych osobowych, które będą przetwarzane, np.* **takie jak imię i nazwisko, częstość skurczów serca i temperatura skóry**>. **Dane te zostaną wykorzystane do** <*określić sposób i zakres przetwarzania danych, np.* **monitorowania tętna i temperatury skóry na stanowiskach zagrożonych wysoką temperaturą, w celu monitorowania wydolności fizjologicznej w ekstremalnie trudnych warunkach pracy**>. **Osobą odpowiedzialną za przetwarzanie danych i ich bezpieczeństwo jest** <*podać imię i nazwisko oraz funkcję osoby odpowiedzialnej, np*. **Jan Kowalski, kierownik działu BHP**>. Dane będą dostępne dla <*podać funkcję osoby/osób, która będzie miała / które będą miały dostęp do danych, np.* **osoba odpowiedzialna za BHP na danej zmianie roboczej**>. **Bezpieczeństwo ochrony danych zagwarantowane jest** <*podać nazwę / sposób identyfikacji systemu informatycznego oraz sposobu wdrożenia stosownych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem, np*. **przez zastosowanie systemu informatycznego X, zapewniającego szyfrowany dostęp do przetwarzanych danych**>.
5. **Oświadczenie pracodawcy** **Dane osobowe będą przetwarzane z zachowaniem postanowień Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (Dziennik Urzędowy UE L 119/1 z 4 maja 2016).**

Zaproponowany wzór oświadczenia pracownika, w którym wyraża on zgodę na przetwarzanie danych osobowych w związku z wykonywaną pracą, zawiera poza samym oświadczeniem pracownika (punkt 1 w tabeli 2) również zwięzłą informację pracodawcy o tym, co jest przedmiotem oświadczenia woli pracownika, jak również oświadczenie pracodawcy, iż dane będą przetwarzane

jedynie w sposób zgodny z obowiązującą ustawą o ochronie danych osobowych. Wzór zaproponowany w tabeli 2 może być modyfikowany w zależności od stanowiska pracy, rodzaju i ilości przetwarzanych danych osobowych oraz pod względem graficznym. W tabeli 3 przedstawiono kolejny wzór oświadczenia, w którym tekst z punktów 1 i 2 umieszczono w formie tabelarycznej.

Tabela 3. Wzór proponowanego oświadczenia pracownika, w którym wyraża on zgodę na przetwarzanie danych osobowych (wzór nr 2)

1.

<Imię i nazwisko> …….. wyrażam zgodę na przetwarzanie następujących danych osobowych:

1)	Imię i nazwisko
2)	Częstość skurczów serca
3)	Temperatura skóry

2.

Zostałem poinformowany przez pracodawcę o:

- rodzaju i formie przetwarzanych danych osobowych,
- sposobie i zakresie przetwarzania tych danych,
- gwarancjach odnoszących się do ochrony przetwarzanych danych.

3.

Data i podpis pracownika

……. ……

4.
Informacje dla pracownika

Stanowisko pracy, na którym będą przetwarzane dane	Piecowy
Rodzaj danych	Tętno, temperatura skóry
Powód przetwarzania danych	Monitorowanie wydolności fizjologicznej w ekstremalnie trudnych warunkach pracy
Osoba odpowiedzialna za przetwarzanie danych	Jan Kowalski, kierownik działu BHP
Gwarancje bezpieczeństwa ochrony danych	Zastosowanie systemu informatycznego X, zapewniającego szyfrowany dostęp do przetwarzanych danych

5.
Oświadczenie pracodawcy
Dane osobowe będą przetwarzane z zachowaniem postanowień Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (Dziennik Urzędowy UE L 119/1 z 4 maja 2016).

Niezależnie od formy, w której oświadczenie zostanie przygotowane, musi ono uwzględniać pełny zakres przetwarzanych danych osobowych oraz być zrozumiałe dla pracownika.

6. Zalecenia w zakresie ochrony danych i zapewnienia cyberbezpieczeństwa

W rozdziale przedstawiono ogólne zalecenia/wytyczne, których przestrzeganie pozwala na zabezpieczenie danych w systemach IoT. Zalecenia mają charakter ogólny, tzn. odnoszą się do wszystkich obszarów IoT. Mogą więc być stosowane również do ochrony danych i zapewnienia cyberbezpieczeństwa w systemach inteligentnych środków ochrony indywidualnej.

Ochrona danych i zapewnienie cyberbezpieczeństwa powinny obejmować wszystkie opisane w rozdziale 2 elementy, na których opiera się obieg danych, czyli: integralność, poufność i dostępność. Chodzi zatem o objęcie ochroną wszystkich elementów architektury bezpieczeństwa danego systemu. W odniesieniu do warstwy percepcyjnej są to głównie zastosowane czujniki, aktuatory itp. W odniesieniu zaś do warstwy transportowej monitorowaniem bezpieczeństwa należy objąć technologie zastosowane do transmisji danych, a – do warstwy aplikacji wszelkie algorytmy i aplikacje pozwalające na gromadzenie, przetwarzanie i dostęp do danych. **Monitorowanie integralności** to głównie nadzór nad jakością danych. **Monitorowanie poufności** polega na śledzeniu okoliczności, w których poufność została naruszona, oraz na przewidywaniu sytuacji, w których może dojść do jej naruszenia. W tym celu śledzi się działania użytkowników systemów zawierających dane. Sprowadza się ono m.in. do rejestracji kierunków transferu danych i informacji oraz sposobów wykorzystywania przez użytkowników zastosowanych w systemie algorytmów i aplikacji. **Monitorowanie dostępności** polega na monitorowaniu dostępności do infrastruktury technicznej oraz oprogramowania, badaniu parametrów określających wydajność i obciążenie systemu, a także sprawdzaniu kompatybilności z innymi współpracującymi systemami.

Aby uniknąć cyberataków, wszystkie instytucje, w których funkcjonują systemy elektroniczne i telekomunikacyjne, muszą zweryfikować, w jaki sposób urządzenia działające w odniesieniu do koncepcji IoT są wdrażane i zabezpieczane[97]**.**

[97] Mitnick K.: *The art of invisibility: The world's most famous hacker teaches you how to be safe in the age of Big Brother and big data*. New York, Hachette Book Group 2017.

W listopadzie 2017 r. został opracowany przez *European Union Agency for Network and Information Security* dokument skupiający się na najważniejszych elementach związanych z cyberbezpieczeństwem IoT i określeniem podstawowych zaleceń z nim związanych[98]. Poniżej wyszczególniono zawarte w nim najważniejsze zalecenia w zakresie cyberbezpieczeństwa i ochrony danych:

1. Częsta aktualizacja oprogramowania urządzeń najnowszym oprogramowaniem i poprawkami możliwie jak najszybciej, aby mieć pewność, że są one odporne na znane luki w zabezpieczeniach.
2. Zmiana domyślnych danych uwierzytelniających (haseł) i ustawień urządzeń. Pozwoli to zabezpieczyć je np. przed atakami polegającymi na skanowaniu Internetu w poszukiwaniu urządzeń akceptujących słabe lub domyślne ustawienia podczas negocjacji połączenia oraz znacznie utrudnić przeprowadzenie ataku na hasło *bruteforce*.
3. Wybieranie wystarczająco długich i złożonych haseł, a nie statycznych i słabych.
4. Prawidłowa konfiguracja zapory (ang. *firewall*) i odfiltrowywanie/blokowanie podejrzanego ruchu. Przykładowo blokowanie przychodzącego ruchu po UDP (ang. *User Datagram Protocol*), ponieważ jest on wykorzystywany do ataków na urządzenia, w tym urządzenia IoT.
5. Odpowiednie śledzenie urządzeń i zarządzanie nimi – dobrym punktem wyjścia do projektowania IoT jest dokładne zrozumienie, jak są połączone urządzenia. W związku z tym zaleca się wdrożenie rozwiązania wykrywania, śledzenia i zarządzania zasobami.
6. Fizyczne zabezpieczanie urządzeń pośredniczących w transmisji przed dostępem do ich zasobów, np. routerów lub switchy.
7. Wykonanie pewnego rodzaju testów penetracyjnych lub oceny urządzeń na poziomie sprzętu lub oprogramowania przed ich wdrożeniem w celu wykrycia luk w zabezpieczeniach.
8. Stosowanie aktualnych protokołów szyfrowania – dane wchodzące i wychodzące z urządzeń powinny być zabezpieczone za pomocą najsilniejszych dostępnych metod szyfrowania.
9. Zabezpieczenie całej transmisji danych najlepiej zarówno na poziomie warstwy transportowej, jak i warstwy aplikacji.
10. Zabezpieczenie/szyfrowanie danych przechowywanych zarówno na urządzeniach końcowych, jak i serwerach.

[98] Baseline Security Recommendations for IoT in the context of Critical Information Infrastructures [online]. European Union Agency For Network And Information Security [dostęp: 19 V 2018]. https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot/at_download/fullReport

11. Przejście od kontroli na poziomie urządzenia do kontroli na poziomie tożsamości – ponieważ coraz więcej urządzeń IoT oferuje możliwość połączenia wielu użytkowników z jednym urządzeniem, troska o bezpieczeństwo powinna koncentrować się na kontroli poziomu tożsamości. Uwierzytelnianie pomaga lepiej zrozumieć, w jaki sposób użytkownik uzyskuje dostęp do urządzenia, oraz może również pomóc w lepszej ochronie przed lukami w zabezpieczeniach i ich niewłaściwym użytkowaniem.
12. Ograniczenia związane z gromadzeniem danych – zbieranie wyłącznie danych potrzebnych do świadczenia usługi i przechowywanie ich tylko przez ograniczony czas.
13. W przypadku transmisji bezprzewodowej ustawienie niezbędnego i wystarczającego poziomu mocy urządzeń aby jej zasięg był pod kontrolą.

Brak zapewnienia bezpiecznego obiegu danych/informacji uniemożliwia skuteczne zarządzanie nimi. Działania w tym zakresie powinny obejmować wszystkie możliwe aspekty, które mogą mieć znaczenie dla prawidłowego zabezpieczenia danych w systemie. Ponieważ monitorowanie bezpieczeństwa danych można podzielić na dwa zasadnicze aspekty (techniczny i społeczny), nie bez znaczenia jest również zwrócenie uwagi na to, czy w samym procesie monitorowania bezpieczeństwa biorą udział odpowiednie osoby. To jeden z najtrudniejszych i najbardziej wrażliwych aspektów w całym procesie związanym z monitorowaniem bezpieczeństwa danych. Nigdy nie można mieć pewności, że osoby odpowiedzialne za bezpieczeństwo danych na określonych etapach ich gromadzenia, przetwarzania lub przesyłania nie okażą się hakerami, dla których bezpośredni dostęp do procedur związanych z monitorowaniem bezpieczeństwa danych będzie tylko ułatwieniem procederu związanego np. z wyciekiem danych wrażliwych. Istotne jest więc również to, aby zapewnić takie procedury monitorowania bezpieczeństwa danych w systemie, aby mógł on również sam siebie monitorować[99].

Z przykładów opisanych w rozdziale 4, odnoszących się również do środowiska pracy, wynika, że dla zapewnienia bezpieczeństwa obiegu danych i informacji w tego typu systemach konieczne jest zastosowanie warstwowej architektury bezpieczeństwa IoT, co wiąże się z koniecznością wprowadzenia niezależnych zabezpieczeń warstw (percepcyjnej, transportowej i warstwy aplikacji).

[99] Bejtlich R.: *The Practice of Network Security Monitoring. Understanding Incident Detection and Response*. San Francisco, No Starch Press, Inc. 2013.

Bibliografia

Alt S., Fouque P.-A., Macario-rat G., Onete C., Richard B.: *A Cryptographic Analysis of UMTS/LTE AKA* [dostęp: 2019-05-29]. https://eprint.iacr.org/2016/371.pdf

Abdelgawad A., Yelamarthi K., Khattab A.: *IoT – Based Health Monitoring System for Active and Assisted Living* [dostęp: 2019-06-14]. http://www.springer.com/cda/content/document/cda_downloaddocument/9783319619484-c2.pdf?SGWID=0-0-45-1611806-p180938434

Banerji S., Chowdhury R. S.: *On IEEE 802.11: Wireless LAN Technology, International Journal of Mobile Network Communications & Telematics* [online]. (IJMNCT) [dostęp: 2019-09-10]. https://arxiv.org/ftp/arxiv/papers/1307/1307.2661.pdf

Baseline Security Recommendations for IoT in the context of Critical Information Infrastructures [online]. European Union Agency For Network And Information Security [dostęp: 19 V 2018]. https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot/at_download/fullReport

Computer Hope [dostęp: 2018-05-10]. https://www.computerhope.com/jargon/d/data.htm

4G, LTE, 3G, 2G – czym różnią się od siebie poszczególne technologie? [online]. Daily Web [dostęp: 2019-05-30]. https://dailyweb.pl/4g-lte-3g-2g-czym-roznia-sie-od-siebie-poszczegolne-technologie/

Data [online]. TechTerms [dostęp: 2018-05-10]. https://techterms.com/definition/data

DNA of IoT [dostęp: 2019-06-28]. https://www.semtech.com/technology/lora

DOBREPROGRAMY [dostęp: 2018-02-15]. https://www.dobreprogramy.pl/macminik/Rynek-mobilnych-gadzetow-sie-rozwija,70723.html

DOKO [dostęp: 2019-06-17]. http://www.dokotech.com/doko/people/

Dziedzic K.: *Wi-Fi bez tajemnic* [online]. Komputer Świat [dostęp: 2019-04-23]. http://www.komputerswiat.pl/jak-to-dziala/2015/06/standardy-wifi.aspx

Ewolucja telefonii komórkowej (1) – czym są sieć 1G, 2G? [online]. Czytelnia Internetowa WBP w Opolu [dostęp: 2019-05-30]. https://internetowaopole.wordpress.com/2018/01/26/krotka-historia-telefonii-komorkowej-w-polsce/

Fischer C., Gellersen H.: *Location and navigation support for emergency responders: a survey* [online]. LOCATION-BASED SERVICES [dostęp: 2019-06-14]. https://core.ac.uk/download/pdf/1549878.pdf

Garmin [dostęp: 2019-06-14]. https://buy.garmin.com/pl-PL/PL/p/548743

Gupta S., Dham R.: *Bluetooth Low Energy 4.2 przynosi większe bezpieczeństwo komunikacji ElektronikaB2B* [online]. ElektronikaB2B [dostęp: 2019-05-27]. https://elektronikab2b.pl/prezentacja-artykul/31341-bluetooth-low-energy-42-przynosi-wieksze-bezpieczenstwo-komunikacji#.WtYchIhuaUk

Heon-june K.: *A study on the Cryptographic Algorithm for NFC* [online]. Indian Journal of Science and Technology 2016, vol. *9*(37) [dostęp: 2019-05-27]. http://www.indjst.org/index.php/indjst/article/viewFile/102543/74044

Hill S.: *4G vs. LTE: The differences explained* [online]. Digital Trends [dostęp: 2019-05-30]. https://www.digitaltrends.com/mobile/4g-vs-lte/

Internet of things, strategic research roadmap [online]. DOCPLAYER [dostęp: 2019-04-17]. https://docplayer.net/11937485-Internet-of-things-strategic-research-roadmap-antoine-de-saint-exupery.html

Kaczmarek S.: *Czy transmisja danych w sieciach LTE jest bezpieczna?* [online]. TELKO.IN [dostęp: 2019-05-30]. https://www.telko.in/czy-transmisja-danych-w-sieciach-lte-jest-bezpieczna,0

Kavya S., Pavithra K., Rajaram S., Vahini M., Harini N.: *Vulnerability Analysis And Security System For NFC-Enabled Mobile Phones*. International Journal Of Scientific & Technology Research 2014, *3*(6) [dostęp: 2019-05-27]. http://www.ijstr.org/final-print/june2014/Vulnerability-Analysis-And-Security-System-For-Nfc-enabled-Mobile-Phones.pdf

Koperski B., Nowak M., Szymborska A.: *Wykorzystanie standardu LoRaWAN do budowy bezprzewodowych sieci-sensorowych w inteligentnych budynkach* [online]. Napędy i Sterowanie 2016, nr 6 [dostęp: 2019-05-29]. http://yadda.icm.edu.pl/baztech/element/bwmeta1.element.baztech-5e1aeff2-041d-4972-9422-3cab08ab23f7/c/NIS-2016-6-Nowak-Wykorzystanie.pdf

LoRaWAN Overview [online]. GitHub [dostęp: 2019-06-28]. https://github.com/Fluent-networks/floranet/wiki/LoRaWAN-Overview

Majchrzyk Ł.: *20. rocznica telefonii komórkowej w Polsce* [online]. MOBIRANK [dostęp: 2019-05-30]. https://mobirank.pl/2016/10/26/20-rocznica-telefonii-komorkowej-polsce/

Mehta R.: *Why Industrial IoT platform is best hope for IT and OT convergence* [online]. CIO [dostęp: 2019-04-17]. https://www.cio.com/article/2977651/predictive-analytics/why-industrial-iot-platform-is-best-hope-for-it-and-ot-convergence.html

Mitnick K.: *The art of invisibility: The world's most famous hacker teaches you how to be safe in the age of Big Brother and big data*. New York, Hachette Book Group 2017.

Mitnick K., Simon W. L.: *Ghost in the Wires. My Adventures as the World's Most Wanted Hacker*. Boston, Little, Brown and Company 2011.

Near Field Communication [dostęp: 2019-05-27]. http://nearfieldcommunication.org/

Netronix [dostęp: 2019-04-23]. http://netronix.pl/pl/informacje/hitag-stabilny-standard-rfid-dla-wymagajacych-aplikacji.htm

Netronix [dostęp: 2019-05-27]. http://netronix.pl/pl/informacje/icode-standard-rfid-dla-aplikacji-hf-1356mhz-wymagajacych-antykolizji.html

802.15.1™. IEEE Standard for Information technology – Telecommunications and information exchange between systems – Local and metropolitan area networks – Specific requirements [online]. New York, NY, The Institute of Electrical and Electronics Engineers, Inc. 2002 [dostęp: 2019-05-27]. http://www.diegm.uniud.it/tonello/MATERIAL/STANDARDS/802.15.1/802.15.1-2002.pdf

Owczarek G.: *Wybór czujników do monitorowania parametrów środowiska pracy i zdrowia pracowników*. W: *Nowe trendy w bezpieczeństwie pracy, środowisku i zarządzaniu*. Pod red. nauk. B. Szczuckiej-Lasoty & W. Kriesera. Katowice, Wyższa Szkoła Zarządzania Ochroną Pracy 2018.

Owczarek G., Gralewicz G.: *Aktywne i pasywne optyczne filtry ochronne – zasada działania, podstawy konstrukcji*. Warszawa, CIOP-PIB 2017.

Padgette J., Scarfone K., Chen L.: *Guide to Bluetooth Security* [online]. National Institute of Standards and Technology U.S. Department of Commerce [dostęp: 2019-05-27]. https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-121r1.pdf

PWSK [dostęp: 2019-05-27]. https://www.pwsk.pl/rfid/tagi-rfid-mifare/

Qi Jing, Vasilakos A. V., Wan J., Jingwei Lu, Dechao Qiu: Security of the Internet of Things: perspectives and challenges. Wireless Networks 2014, vol. 20, issue 8.

Sapronov K.: *Bluetooth i problemy z bezpieczeństwem* [online]. Securelist [dostęp: 2019-05-27]. https://securelist.pl/threats/5548,bluetooth_i_problemy_z_bezpieczenstwem.html

Stallings W.: *Cryptography and Network Security. Principles and Practice*. Pearson Education Limited, London 2016.

Textiles and textile products – Smart textiles – Definitions, categorisation, applications and standardization needs [online]. NSAI Standards. Standard Recommendation S.R. CEN/TR 16298:2011 [dostęp: 2019-05-31]. https://infostore.saiglobal.com/preview/is/en/2011/srcen-tr16298-2011.pdf?sku=1505398

UnitagNFC [dostęp: 2019-05-27]. https://www.unitag.io/nfc/what-is-nfc

Vermesan O., Friess P.: Internet of Things – From Research and Innovation to Market Deployment [online]. River Publishers 2014 [dostęp: 2019-04-17]. http://www.internet-of-things-research.eu/pdf/IERC_Cluster_Book_2014_Ch.3_SRIA_WEB.pdf

Wilson G.: *Przetwarzanie danych dla programistów*. [Tł. M. Pętlicki]. Gliwice, Wydawnictwo HELION 2006.

Dyrektywa 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych.

Ustawa z dn. 29 sierpnia 1997 r. o ochronie danych osobowych (DzU 1997, nr 133, poz. 883).

Załącznik 1

Normy międzynarodowe i inne dokumenty w zakresie cyberbezpieczeństwa

W celu zapewnienia cyberbezpieczeństwa opracowano wiele metodyk, wytycznych i poradników, które pomagają we wdrożeniu dobrych praktyk w zakresie zapewnienia możliwie wysokiego poziomu cyberbezpieczeństwa. Poniżej zestawienie i krótka charakterystyka najważniejszych dokumentów tego typu:

ITIL (*Information Technology Infrastructure Library – Security Management*) – wytyczne w zakresie kontroli poziomu cyberbezpieczeństwa, zarządzanie incydentami związanymi z cyberbezpieczeństwem, prowadzenia audytów weryfikujących skuteczność kontroli poziomu cyberbezpieczeństwa, monitorowania skuteczności zabezpieczeń.

NIST (*National Institute of Standards and Technology*) SP 800-115 – przewodnik techniczny do przeprowadzania testów bezpieczeństwa.

ISM3 (*Information Security Management Maturity Model*) – wytyczne do oceny własnego środowiska pracy oraz wytyczne umożliwiające zaplanowanie procesów zarządzania bezpieczeństwem, aby zapewnić efektywną realizację celów biznesowych organizacji.

OSSTMM (*Open Source Security Testing Methodology Manual*) – recenzowany podręcznik testowania i analizy zabezpieczeń.

ISSAF (*Information Systems Security Assessment Framework*) – metodyka OISSG (*Open Information Systems Security Group*) w zakresie weryfikacji strategii bezpieczeństwa.

OWASP (*The Open Web Application Security Project*) – metodyka prowadzenia testów penetracyjnych.

WASC (*Web Application Security Consortium*) – opracowywanie i propagowanie standardów bezpieczeństwa w Internecie.

Funkcjonują również normy międzynarodowe dotyczące cyberbezpieczeństwa (publikowane także w wersji polskiej). Poniżej zestawienie i ich krótka charakterystyka:

1. ISO/IEC 27000:2016 *Information technology – Security techniques – Information security management systems – Overview and vocabulary*. Wersja polska PNISO/IEC 27000:2017-06 *Technika informatyczna – Techniki bezpieczeństwa – Systemy zarządzania bezpieczeństwem informacji – Przegląd i terminologia.*

Norma zawiera przegląd systemów zarządzania bezpieczeństwem informacji oraz 89 terminów i ich definicje powszechnie stosowane w normach dotyczących cyberbezpieczeństwa. Ma zastosowanie w organizacjach różnego typu (niezależnie od wielkości), np. przedsiębiorstwach handlowych, agencjach rządowych, organizacjach typu non profit.

2. ISO/IEC 27001:2017 *Information technology. Security information. Security management systems. Requirements*. Wersja polska PN-ISO/IEC 27001:2017-06 *Technika informatyczna – Techniki bezpieczeństwa – Systemy zarządzania bezpieczeństwem informacji – Wymagania*.

   Norma prezentuje model Systemu Zarządzania Bezpieczeństwem Informacji (SZBI) oraz metodę jego ustanowienia, wdrożenia, eksploatacji, monitorowania, przeglądu, utrzymania i doskonalenia.

3. ISO/IEC 27002:2017 *Information technology. Security techniques. Code of practice for information security controls*. Wersja polska PN-EN ISO/IEC 27002:2017-06 *Technika informatyczna – Techniki bezpieczeństwa – Praktyczne zasady zabezpieczania informacji*.

   Norma umożliwiająca opracowanie skutecznego SZBI. Omawia cele stosowania zabezpieczeń oraz opisuje metody ich wdrażania na podstawie oszacowanego ryzyka (133 zasady dotyczące bezpieczeństwa informacji).

4. ISO/IEC 27003:2017 *Information technology – Security techniques. Information security management systems. Guidance*.

   Norma wskazuje na kluczowe aspekty niezbędne do skutecznego zaprojektowania i wdrożenia SZBI. Określa proces specyfikacji SZBI od momentu projektowania do opracowania planów wdrożeniowych. Opisuje także proces uzyskania akceptacji kierownictwa na wdrożenie SZBI oraz podaje wytyczne dotyczące planowania SZBI i jego realizacji.

5. PN-ISO/IEC 27004:2017-07 *Information technology. Security techniques. Information security management. Measurement, monitoring, measurement, analysis and evaluation*. Wersja polska PN-ISO/IEC 27004:2017-07 *Technika informatyczna – Techniki bezpieczeństwa – Zarządzanie bezpieczeństwem informacji – Monitorowanie, pomiary, analiza i ocena*.

   Norma zawiera wytyczne dotyczące rozwoju i wykorzystywania środków pomiaru w celu oceny skuteczności wdrożenia SZBI, a także wytyczne mające pomóc organizacjom w ocenie wyników dotyczących bezpieczeństwa informacji i skuteczności systemu zarządzania nim w celu spełnienia wymagań normy ISO/IEC 27001. Dokument odnosi się do: monitorowania i pomiaru wyników dotyczących bezpieczeństwa informacji; monitorowania i pomiaru skuteczności SZBI, włączając w to jego procesy i zabezpieczenia; analizy i oceny wyników monitorowania i pomiarów. Niniejszy dokument ma zastosowanie do organizacji wszystkich typów i wielkości.

6. ISO/IEC 27005:2014 *Information technology – Security techniques – Information security risk management*. Wersja polska PN-ISO/IEC 27005:2014-01 *Technika informatyczna – Techniki bezpieczeństwa – Zarządzanie ryzykiem w bezpieczeństwie informacji*.

   Norma zawiera wytyczne do zarządzania ryzykiem dotyczącym bezpieczeństwa informacyjnego. Stanowi rozwinięcie ogólnych koncepcji opisanych w PN-ISO/IEC 27001. Jej cele jest wsparcie wdrażania systemu cyberbezpieczeństwa, bazującego na biznesowym podejściu do zarządzania ryzykiem. Ma zastosowanie do wszystkich typów organizacji (np. przedsiębiorstw, instytucji rządowych, organizacji non profit), które powinny

uwzględniać zarządzanie ryzykiem, aby uniknąć naruszania procedur bezpieczeństwa w ramach doskonalenia SZBI.

7. ISO/IEC 27006:2016 *Information technology – Security techniques – Requirements for bodies providing audit and certification of information security management system*. Wersja polska PN-ISO/IEC 27006:2016-12 *Technika informatyczna – Techniki bezpieczeństwa – Wymagania dla jednostek prowadzących audyt i certyfikację systemów zarządzania bezpieczeństwem informacji*.

   Norma określa wymagania i wytyczne dla jednostek prowadzących audyt i certyfikację SZBI. Może być stosowana do celów audytu wewnętrznego SZBI. Stanowi uzupełnienie wymagań zamieszczonych w ISO/IEC 27001.

8. ISO/IEC 27007:2017 *Information technology – Security techniques – Guidelines for information security management systems auditing*. Wersja polska PN-ISO/IEC 27007:2017-06 *Technologia informacyjna – Techniki bezpieczeństwa – Wytyczne dotyczące audytu systemów zarządzania bezpieczeństwem informacji*.

   Norma zawiera wytyczne dotyczące zarządzania programem audytu SZBI i zasad ich przeprowadzania oraz określa kompetencje audytorów. Odnosi się do osób, które mogą prowadzić audyty wewnętrzne i zewnętrzne SZBI. Jest uzupełnieniem normy ISO 19011:2011, określającej zasady prowadzenia audytu dowolnego systemu zarządzania.

9. ISO/IEC 27010:2015 *Information technology – Security techniques – Information security management for inter-sector and inter-organisational communications*.

   Norma stanowi uzupełnienie wytycznych podanych w normach serii ISO/ IEC 27000 dotyczących wdrażania zarządzania bezpieczeństwem informacji w organizacjach wspólnie zarządzających zasobami informacyjnymi. Zawiera zalecenia odnoszące się do inicjowania, wdrażania, utrzymania i poprawy bezpieczeństwa informacji w ramach komunikacji między organizacjami i sektorami. Ma zastosowanie do wszystkich form wymiany informacji i służy do udostępniania informacji poufnych, zarówno publicznych, jak i prywatnych, krajowych i międzynarodowych, w ramach tego samego sektora przemysłu lub rynku lub między sektorami. W szczególności zasady te mogą być stosowane do wymiany informacji i wiedzy z zakresu dostarczania, utrzymywania i ochrony infrastruktury krytycznej danej organizacji. Celem normy jest wspieranie i kreowanie zaufania podczas wymiany i udostępniania poufnych informacji, a tym samym sprzyjanie rozwojowi międzynarodowej wymiany informacji społecznościowych.

10. ISO/IEC 27011:2008 *Information technology – Security techniques – Information security management guidelines for telecommunications organizations based on ISO/IEC 27002*.

    Norma określa wytyczne wspierające wdrażanie zarządzania cyberbezpieczeństwem w organizacjach telekomunikacyjnych. Umożliwia organizacji telekomunikacyjnej spełnienie podstawowych wymogów w zakresie zarządzania cyberbezpieczeństwem, czyli zapewnienie poufności, integralności i dostępności oraz innych istotnych atrybutów cyberbezpieczeństwa.

11. ISO/IEC 27013: 2015 *Guidance on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1*. Wersja polska PN-ISO/IEC 27013:2014-01 Technika informatyczna – Techniki bezpieczeństwa – Wytyczne do zintegrowanego wdrożenia ISO/IEC 27001 oraz ISO/IEC 20000-1.

Norma zawiera wytyczne dotyczące zintegrowanego systemu zarządzania cyberbezpieczeństwem, opartego na ISO/IEC 27001, oraz systemu zarządzania usługami informatycznymi, którego wymagania określono w normie ISO/IEC 20000-1. Norma ma zastosowanie w organizacjach zamierzających wdrożyć zintegrowany system zarządzania uwarunkowany wyżej wymienionymi normami.

12. ISO/IEC 27014:2015 Information technology – Security techniques – Governance of information security.

    W normie przedstawiono wytyczne dotyczące określania pojęć i zasad zarządzania bezpieczeństwem informacji, dzięki którym organizacje mogą kształtować tzw. ład informatyczny uwzględniający zagadnienia związane z cyberbezpieczeństwem. Ma zastosowanie do wszystkich typów i rozmiarów organizacji.

13. ISO/IEC 27018:2017 *Information technology Security techniques – Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processor.* Wersja polska PN-ISO/IEC 27018:2017-07 *Technika informatyczna – Techniki bezpieczeństwa – Praktyczne zasady ochrony danych identyfikujących osobę* (PII – *personally identifiable information*) *w chmurach publicznych działających jako przetwarzający PII*.

    Norma ustanawia powszechnie uznawane cele stosowania zabezpieczeń, zabezpieczenia oraz wytyczne do wdrażania środków ochrony danych identyfikujących osobę dla środowiska przetwarzania w chmurze.

Załącznik 2

Słownik najważniejszych terminów używanych w obszarze bezpieczeństwa obiegu danych i informacji w systemach Internetu rzeczy

1. **AES** (ang. *Advanced Encryption Standard*) – symetryczny szyfr blokowy, który od roku 2001 jest obecnym standardem kryptograficznym służącym do szyfrowania danych.

2. **Aktuator** – element/urządzenie/organ wykonawczy, którym może być np. siłownik, silnik oraz także palec, dłoń, ręka czy noga człowieka.

3. **Architektura bezpieczeństwa** – ujednolicony projekt zabezpieczeń, który uwzględnia potrzeby i potencjalne zagrożenia związane z określonym scenariuszem lub środowiskiem. Określa również, kiedy i gdzie stosować zabezpieczenia. Proces projektowania jest zasadniczo powtarzalny. W architekturze bezpieczeństwa zasady projektowania są jasno opisane, a szczegółowe specyfikacje kontroli bezpieczeństwa zazwyczaj dokumentowane w niezależnych dokumentach.

4. **Atak hakerski** – działalność polegająca na nielegalnym korzystaniu z komputera w celu uzyskania w sposób nieautoryzowany dostępu do informacji, najczęściej osobistych, przechowywanych w innym systemie komputerowym, lub do rozprzestrzeniania wirusa komputerowego.

5. **Biometria** – nauka zajmująca się badaniem zmienności populacji organizmów przez badanie ich cech fizycznych (np. linie papilarne, siatkówka oka) oraz cech behawioralnych związanych z zachowaniem (np. podpis odręczny, sposób chodzenia). Jest również techniką dokonywania pomiarów istot żywych. Obecnie wykorzystywana jest głównie jako sposób kontroli dostępu do chronionych pomieszczeń lub autoryzacji użytkowników korzystających z określonych danych, programów czy urządzeń.

6. **BLE** (ang. *Bluetooth Low Energy*) – technologia bezprzewodowej komunikacji pomiędzy różnymi urządzeniami elektronicznymi wykorzystująca do przesyłania danych fale radiowe. W porównaniu ze standardową technologią Bluetooth charakteryzuje się głównie niższym

zużyciem energii kosztem krótszego zasięgu – do 30 metrów. Obecnie powszechnie stosowana jest do łączenia wszelkiego typu urządzeń komunikujących się ze smartfonem.

7. **Bluetooth** – standard bezprzewodowej komunikacji na nieduże odległości, do 100 metrów. Umożliwia przesyłanie danych pomiędzy urządzeniami, takimi jak: laptopy, telefony komórkowe, zestawy słuchawkowe, tablety itd.

8. **Brama/Gateway** – węzeł sieciowy, oprogramowanie lub sprzęt łączący dwie odmienne sieci komputerowe, który umożliwia przepływ informacji między siecią domową lub firmową a Internetem.

9. **Dostępność** – jedna z podstawowych właściwości bezpieczeństwa informacji. W kontekście systemu komputerowego dotyczy możliwości uzyskania przez użytkownika na żądanie dostępu do informacji lub zasobów w określonej lokalizacji w dowolnym momencie i w założonym czasie.

10. **EDGE** (ang. *Enhanced Data Rates for GSM Evolution*) – standard pakietowej transmisji danych stosowany w telefonii 2G, który jest rozszerzeniem dla technologii GPRS. Umożliwia przesyłanie danych z szybkością do 236 kb/s (choć teoretycznie nawet do 296).

11. **GPRS** (ang. *General Packet Radio Service*) – standard pakietowej transmisji danych stosowany w telefonii GSM drugiej generacji. Umożliwia przesyłanie danych teoretycznie z szybkością do 100 kb/s, natomiast w praktyce jest to około 30-80 kb/s.

12. **GPS** (ang. *Global Positioning System*) – ogólnoświatowy system nawigacji satelitarnej.

13. **Haker** – osoba mająca bardzo dużą wiedzę informatyczną, która szuka i ewentualnie wykorzystuje luki w zabezpieczeniach systemów informatycznych.

14. **HSPA** (ang. *High Speed Packet Access*) – standard transmisji danych stosowany w telefonii 3G, umożliwiający pobieranie danych z szybkością do 14,4 Mb/s i wysyłanie do 5,7 Mb/s.

15. **Integralność** – jedna z podstawowych właściwości bezpieczeństwa informacji. Zarówno w technice telekomunikacyjnej, jak i bezpieczeństwie teleinformatycznym ochrona integralności zapobiega celowemu lub przypadkowemu zniekształceniu danych podczas transmisji, odczytu czy zapisu danych. Wykorzystuje się do tego celu różnego rodzaju techniki

kryptograficzne, jak mechanizmy do detekcji błędów (sumy kontrolne), kody korekcyjne czy też kody uwierzytelnienia wiadomości.

16. **Inteligentne Produkty** – koncepcja Inteligentnego Produktu wciąż ewoluuje z uwagi na to, że łączy w sobie wiele dyscyplin i może być wykorzystywana na wiele sposobów. Jedną z cech „inteligencji" produktu jest zdolność przetwarzania danych i informacji.

17. **IPsec** (ang. *Internet Protocol Security*, *IP Security*) – zestaw protokołów zapewniających bezpieczeństwo przesyłania danych przez szyfrowanie, uwierzytelnianie oraz bezpieczną wymianę kluczy kryptograficznych.

18. **IrDA** (ang. *Infrared Data Association*) – standard transmisji danych działający w zakresie podczerwieni. Obecnie zrezygnowano z jego wykorzystywania ze względu na jego praktyczność, tzn. w celu transmisji danych anteny nadajnika i odbiornika musiały być skierowane bezpośrednio do siebie i musiały się ze sobą „widzieć" – nie mogło być przeszkód, np. w postaci ścian, mebli itp.

19. **LoRaWAN** (ang. *Long Range Wireless Network*) – stosunkowo nowy standard komunikacji bezprzewodowej przeznaczony głównie do zastosowań Internetu rzeczy (IoT), którego głównym celem jest realizacja komunikacji na bardzo duże odległości (zasięg działania w środowisku miejskim do 5 km, a w terenie otwartym do 15 km) przy bardzo niskim zużyciu energii. Głównym ograniczeniem tej technologii jest dość mała szybkość transmisji danych, wynosząca od 0,3 do 50 Kbps.

20. **LTE** (ang. *Long Term Evolution*) – standard bezprzewodowego transferu danych dla sieci telefonii komórkowej 4G, który teoretycznie pozwala osiągać szybkość transmisji rzędu 300 Mbit/s w przypadku odbierania danych i ok. 80 Mbit/s w przypadku wysyłania.

21. **MIMO** (ang. *Multiple Input, Multiple Output*) – metoda zwiększająca przepustowość sieci bezprzewodowej, polegająca na zastosowaniu transmisji wieloantenowej zarówno po stronie nadawczej, jak i po stronie odbiorczej.

22. **Model OSI** (ang. *Open Systems Interconnection Reference Model*) – model zdefiniowany przez międzynarodową organizację normalizacyjną ISO. Dzięki zbiorowi reguł i standardów oraz podziale na siedem warstw umożliwia komunikację różnego rodzaju systemów i urządzeń, które bazują na tym modelu.

23. **MQTT** (ang. *MQ Telemetry Transport*) – lekki protokół transmisji danych, który m.in. dzięki niskiemu zapotrzebowaniu względem zasobów sieciowych oraz sprzętowych ma zastosowanie głównie w Internecie rzeczy (IoT) i urządzeniach mobilnych.

24. **NFC** (ang. *Near Field Communication*) – technologia bezprzewodowej komunikacji na bliskie odległości – do kilku centymetrów, bazująca na rozwiązaniach technologicznych RFID. Umożliwia połączenie dwóch urządzeń elektronicznych, z których jedno jest zwykle urządzeniem przenośnym (np. smartfon), w celu nawiązania komunikacji przez ich zetknięcie lub ustawienie w odległości kilku centymetrów od siebie. Obecnie ma głównie zastosowanie w autoryzacji transakcji przy płatnościach zbliżeniowych lub transmisji danych (np. wymiana zdjęć „zbliżeniowo" pomiędzy dwoma smartfonami). Uwzględniając wszystkie technologie bezprzewodowe krótkiego zasięgu, NFC uznawane jest za najbardziej bezpieczne.

25. **Oprogramowanie** – w sensie najbardziej ogólnym jest zbiorem instrukcji lub programów instruujących komputer do wykonywania określonych zadań. Oprogramowanie jest ogólnym terminem używanym do opisu programów komputerowych, takich jak: skrypty, aplikacje, programy czy zestawy instrukcji.

26. **Poufność** – jedna z podstawowych właściwości bezpieczeństwa informacji, która mniej więcej równoznaczna jest z prywatnością. Środki podejmowane w celu zapewnienia poufności mają na celu uniemożliwienie dotarcia wrażliwych informacji do nieuprawnionych osób/podmiotów, przy jednoczesnym zapewnieniu, że właściwe osoby/podmioty mogą ten dostęp uzyskać. W bezpieczeństwie teleinformatycznym poufność realizowana jest głównie przy pomocy szyfrowania oraz kontroli dostępu.

27. **RFID** (ang. *Radio-frequency identification*) – jedna z najpopularniejszych technologii krótkiego zasięgu, od kilkunastu centymetrów do kilkunastu metrów, wykorzystująca fale radiowe do transmisji danych. Ma zastosowanie m.in. w identyfikacji osób i przedmiotów na odległość.

28. **Sensor** (czujnik) – urządzenie, którego zadaniem jest wykrywanie sygnałów z otaczającego, fizycznego środowiska, takich jak np.: światło, ciepło, ruch, wilgoć czy ciśnienie.

29. **Serwer** – program komputerowy lub urządzenie, którego zadaniem jest m.in. udostępnianie danych i zasobów, jak np. strony WWW, poczta e-mail, pliki itp., innym programom lub urządzeniom (klientom) podłączonym do sieci komputerowej.

30. **Sieć komputerowa** – zbiór połączonych ze sobą komputerów i innych urządzeń (np. smartfonów, drukarek sieciowych, urządzeń pośredniczących: przełączników, routerów) komunikujących się ze sobą za pomocą różnego rodzaju medium transmisji (skrętka, światłowód, bezprzewodowo), które wykorzystują do tego celu odpowiednie protokoły komunikacyjne.

31. **SSL** (ang. *Secure Socket Layer*) – jeden z najpopularniejszych protokołów, który wykorzystuje szyfrowanie do zabezpieczenia transmisji przesyłanych danych w sieci Internet. Jest częścią protokołu HTTPS.

32. **System komputerowy** – kompletny i funkcjonalny komputer, wraz z całym sprzętem i oprogramowaniem niezbędnym do tego, aby być funkcjonalnym dla użytkownika. Umożliwia użytkownikom wprowadzanie i przechowywanie danych oraz manipulowanie danymi. Systemy komputerowe zazwyczaj obejmują komputer, monitor, klawiaturę, mysz i inne opcjonalne komponenty.

33. **TCP** (ang. *Transmission Control Protocol*) – niezawodny, strumieniowy i połączeniowy protokół kontroli transmisji danych. Na ogół współpracuje z protokołem IP (Internet Protocol), definiując sposób, w który komputery przesyłają pakiety danych do siebie nawzajem.

34. **TLS** (ang. *Transport Layer Security*) – standard, który jest rozwinięciem protokołu SSL, a którego rolą jest zabezpieczenie transmisji przesyłanych danych w sieci Internet. Zapewnia poufność, integralność transmisji danych oraz uwierzytelnienie serwera klienta. Jest częścią protokołu HTTPS.

35. **UMTS** (ang. *Universal Mobile Telecommunications System*) – najpopularniejszy standard transmisji danych stosowany w telefonii 3G, zwany również Uniwersalnym Systemem Telekomunikacji Ruchomej. Umożliwia wykonywanie połączeń głosowych, wideorozmów, wysyłanie wiadomości tekstowych oraz przesyłanie danych z szybkością do 384 kb/s.

36. **Urządzenie mobilne** – urządzenie elektroniczne wystarczająco małe, aby je trzymać i operować nim w dłoni/dłoniach, pozwalające na odbieranie, przetwarzanie oraz wysyłanie danych na ogół bezprzewodowo. Przykładem urządzenia mobilnego może być smartfon, tablet itp.

37. **Wi-Fi** – jedna z najbardziej powszechnie stosowanych technologii bezprzewodowych oparta na łączności radiowej, określana również jako zbiór standardów z rodziny IEEE 802.11 służących do tworzenia lokalnej bezprzewodowej sieci komputerowej. Najczęściej kojarzona jest

z bezprzewodowym dostępem do Internetu w miejscach publicznych, lotniskach, hotelach itp. W mieszkaniach, domach zwykle zabezpieczona jest hasłem dostępu.

38. **WLAN** (ang. *Wireless Local Area Network*) – bezprzewodowa sieć lokalna, sieć w której połączenie dwóch lub więcej urządzeń sieciowych zrealizowane jest bez wykorzystania okablowania a dostęp do Internetu odbywa się przez punkt dostępu (*Access Point*).

39. **WPA2** (ang. *Wi-Fi Protected Access II*) – najmocniejszy obecnie protokół/standard w sieciach bezprzewodowych, który zapewnia największe bezpieczeństwo podczas m.in. transmisji danych dzięki zastosowaniu najmocniejszych algorytmów kryptograficznych takich jak AES.