STUDIA INFORMATICA 2012
Volume 33 Number 2B (106)

Zygmunt MAZUR, Hanna MAZUR
Politechnika Wrocławska, Instytut Informatyki

ROZWÓJ SYSTEMÓW AUTOMATYCZNEJ IDENTYFIKACJI OBIEKTÓW

Streszczenie. Zainteresowanie systemami automatycznej identyfikacji obiektów z wykorzystaniem kodów kreskowych, technologii radiowej RFID i metod biometrycznych jest obecnie bardzo duże i systematycznie rośnie. Wdrażanie ich przynosi wymierne korzyści – obniża koszty pracy, przyspiesza i ułatwia obsługę klientów, zapobiega fałszerstwom i kradzieżom, umożliwia identyfikację obiektów przemieszczających się oraz w miejscach niedostępnych. Niezbędne jest jednak opracowanie odpowiednich standardów i przepisów prawnych. Wykorzystywanie technologii identyfikacyjnych i uwierzytelniających nie byłoby możliwe, gdyby jednocześnie nie powstawały odpowiednie systemy informatyczne (bazy danych wraz z ich oprogramowaniem). W artykule przedstawiono zagadnienia związane z rozwojem systemów automatycznej identyfikacji w aspekcie nowych zastosowań, przetwarzania oraz bezpieczeństwa gromadzonych danych.

Słowa kluczowe: automatyczna identyfikacja, bezpieczeństwo, dane biometryczne, kod kreskowy, identyfikacja RFID

THE DEVELOPMENT OF AUTOMATIC OBJECT IDENTIFICATION SYSTEMS

Summary. The interest in automatic object identification with the use of bar codes, RFID technology and biometric methods is now quite significant and keeps growing. Deployment of these technologies and methods brings numerous advantages: lower costs of running a business, quicker and easier customer service, theft and forgery prevention, possibility for identification of moving objects and objects in inaccessible areas. This, however, requires development of relevant standards, legal regulations, and IT systems (databases with software). This paper presents issues related to the development of automatic object identification systems in the context of new applications, data processing and security of stored data.

Keywords: automatic identification, security, biometric data, bar code, RFID identification

1. Wstęp

Zastosowanie systemów automatycznej identyfikacji[1] towarów, osób i zwierząt przeżywa obecnie prawdziwy rozkwit. Prace badawcze w tym zakresie prowadzone są w wielu ośrodkach naukowych na całym świecie.

W celu przyspieszenia czynności identyfikacyjnych i weryfikacyjnych oraz zwiększenia ich niezawodności, stale ulepszane są i rozwijane metody identyfikacji z wykorzystaniem kodów kreskowych, technologii radiowej RFID (*Radio Frequency Identification*) oraz technik biometrycznych. Efekty wprowadzania tych technologii są bardzo wymierne – obniżenie kosztów pracy, redukcja etatów (np. kasjerów, kontrolerów, urzędników, magazynierów), zwiększenie wydajności pracy, przyspieszenie obsługi klientów, możliwość automatycznej kontroli w warunkach trudnych i niedostępnych itd. Uwierzytelnianie i identyfikacja nie byłyby jednak możliwe do tak szerokiego (masowego) wykorzystania bez odpowiednich baz danych i oprogramowania.

Zbieranie danych biometrycznych i niektóre zastosowania RFID wzbudzają kontrowersje, gdyż istnieją uzasadnione obawy, że wraz z wprowadzeniem nowych rozwiązań identyfikacyjnych na szeroką skalę, bezpowrotnie zostanie utracona prywatność obywateli oraz kontrola nad gromadzeniem i przetwarzaniem ich danych.

W artykule przedstawiono zagadnienia związane z rozwojem systemów automatycznej identyfikacji oraz przykłady zastosowań technologii RFID w aspekcie bezpieczeństwa danych, ze szczególnym uwzględnieniem problemu ochrony prywatności.

2. Kody kreskowe

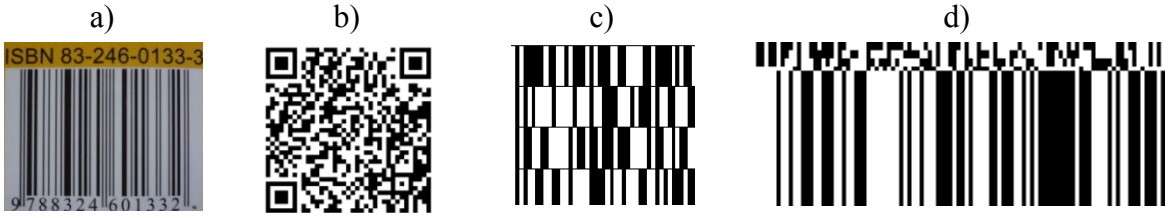
Kody kreskowe, czyli graficzne zapisy danych za pomocą ciemnych i jasnych elementów, wykorzystywane są do oznaczania towarów i urządzeń (nawet bardzo małych, np. układów scalonych), przesyłek, dokumentów (np. faktur, dowodów rejestracyjnych), książek (przez zakodowany ISBN[2], którego przykład przedstawiono na rys. 1a) czy wydawnictw ciągłych (zakodowany ISSN[3]). Dotychczas opracowano około 400 rodzajów kodów [7]. Klasyfikując je, uwzględnia się różne kryteria, na przykład: liczbę wymiarów kodu, szerokości kresek, ciągłość, metody weryfikacji odczytywanych danych, liczbę kodowanych symboli (stałej lub zmiennej długości) lub ich rodzaj (numeryczne – z kodowanymi tylko cyframi w systemie dziesiętnym, lub alfanumeryczne – z kodowanymi znakami ASCII i innych alfabetów). Dane

[1] Automatyczna identyfikacja (ang. *automatic identification*) jest często oznaczana w skrócie AutoID.
[2] ISBN (*International Standard Book Number*) – Międzynarodowy Znormalizowany Numer Książki.
[3] ISSN (*International Standard Serial Number*) – Międzynarodowy Znormalizowany Numer Wydawnictwa Ciągłego.

odczytane z kodu przez czytnik elektroniczny techniką skanowania są przesyłane do systemu komputerowego.

Początkowo (lata 1974 – 1984) wykorzystywano tylko kody jednowymiarowe (linearne), przedstawiane w formie czarno-białych pasków o różnej szerokości (wysokość pasków nie ma znaczenia). Przykładami kodów jednowymiarowych są: Code 128 (do opisu opakowań zbiorczych), Code 39 (wykorzystywany w sektorze medycznym, meblowym, w wojsku i w administracji), przeplatany ITF (*Interleaved Two of Five*) – do znakowania opakowań zbiorczych, EAN-13[4] i EAN-8, UPC-A[5] i UPC-E. Po wielu latach wprowadzono kody dwuwymiarowe (macierzowe i wielowierszowe) oraz hybrydowe (rys. 1d), na przykład RSS, Aztec Mesas, w których można zapisać znacznie więcej danych. Przykładem kodu dwuwymiarowego jest kod matrycowy QR Code (*Quick Response*) przedstawiony na rys. 1b lub wielowierszowy (piętrowy) Code 49 (rys. 1c). Inne popularne kody dwuwymiarowe to DataMatrix (kod o zmiennej długości, wykorzystywany np. w logistyce do oznaczania dokumentów i urządzeń elektronicznych), kod o dużej gęstości zapisu PDF-417 (*Portable Data File*), Aztec Code (przypominający wyglądem aztecką piramidę), MaxiCode – przedstawiany zawsze jako kwadrat o boku 1 cala, przeznaczony między innymi do znakowania przedmiotów w miejscach zgiętych lub będących w ruchu (np. przesuwanych na taśmie produkcyjnej).

Zastosowanie kodów kreskowych do znakowania wymaga jednocześnie odpowiedniego oprogramowania umożliwiającego gromadzenie danych o produktach, ich identyfikację i wykonywanie wymaganych procesów biznesowych, takich jak np. zamówienie towaru, dostawa, sprzedaż, wycofanie, przecena, reklamacja itd.



Rys. 1. Przykładowe kody kreskowe: a) jednowymiarowy EAN-13, b) matrycowy QR, c) wielowierszowy Code 49, d) hybrydowy

Fig. 1. Example bar codes: a) one-dimensional EAN-13, b) matrix QR Code, c) stacked Code 49, d) hybrid

Posługiwanie się kodami kreskowymi znacznie przyspiesza wiele prac magazynowych, handlowych czy logistycznych, jednak wymaga bezpośredniego zbliżenia kodu do czytnika (kod musi być widoczny). Opakowania zawierające większe ilości towarów czy dokumenty z umieszczonym wewnątrz kodem kreskowym, muszą być otwierane w celu uwidocznienia kodu podczas odczytu, co utrudnia i spowalnia prace oraz uniemożliwia ich automatyzację.

[4] EAN (*European Article Number*) – Europejski Kod Towarowy, EAN-13 jest kodowany za pomocą 12 cyfr i jednej cyfry kontrolnej, a EAN-8 za pomocą 7 cyfr i jednej cyfry kontrolnej.

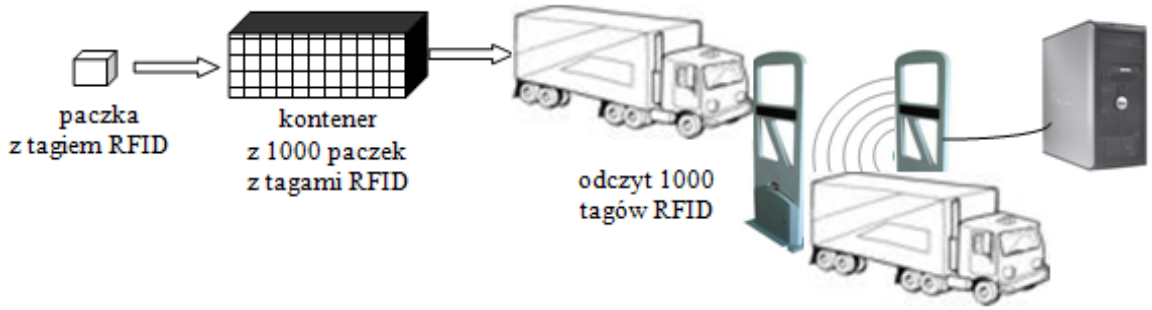
[5] UPC (*Universal Product Code*) – Uniwersalny Kod Produktów, UPC-A jest kodowany za pomocą 12 cyfr, a UPC-E za pomocą 6 cyfr.

Znacznie wygodniejszym rozwiązaniem jest coraz powszechniej wykorzystywana technologia RFID.

3. Identyfikacja RFID

Do identyfikacji obiektów w technologii RFID wykorzystywane są urządzenia elektroniczne, zwane transponderami, oraz czytniki[6] komunikujące się z nimi za pomocą fal radiowych o odpowiedniej częstotliwości[7]. Każdy transponder ma przypisany jednoznaczny kod i w zależności od rodzaju może być wykorzystywany do odczytu, usunięcia i/lub zapisu danych. Transpondery mogą być ukryte, zanieczyszczone oraz znajdować się w określonej odległości od czytnika, a ich identyfikacja jest nadal niezawodna i może być wykonywana automatycznie. Z tego względu zyskują coraz większą popularność i wypierają kody kreskowe.

Transponder RFID, nazywany również tagiem lub znacznikiem, składa się z mikrochipu z pamięcią przechowującą dane (m.in. unikalny numer transpondera) i z anteny, która często ma postać niewielkich rozmiarów wielozwojowej cewki. Tak zbudowany transponder zwany jest pasywnym (ang. *passive*), gdyż oczekuje na sygnał pochodzący od czytnika i również z niego czerpie energię niezbędną do działania. Przesłanie danych drogą radiową z transpondera pasywnego do czytnika następuje, gdy znajdzie się on w jego polu magnetycznym. Czytnik RFID (ang. *RFID reader* lub *interrogator*), który składa się z nadajnika, odbiornika, dekodera i anteny nadawczo-odbiorczej (lub nadawczej i odbiorczej), po zweryfikowaniu poprawności danych (przez porównanie z sumą kontrolną), przekazuje je do systemu komputerowego w celu zidentyfikowania obiektu. Dzięki temu, że odpowiedź transpondera na otrzymany sygnał z czytnika nie jest natychmiastowa i po jej udzieleniu transponder pozostaje przez pewien czas bezczynny, możliwy jest odczyt z wielu tagów jednocześnie. Schemat działania systemu RFID przedstawiono na rysunku 2.



Rys. 2. Schemat działania systemu identyfikacji RFID
Fig. 2. A scheme of an RFID-based object identification system

[6] Często są to urządzenia czytająco-zapisujące.
[7] LF (*Low Frequency*) – 125/134,2 kHz, HF (*High Frequency*) – 13,56 MHz, VHF (*Very High Frequency*) – 30-300 MHz, UHF (*Ultra High Frequency*) – 860-960 MHz, Microwave – 2,4/5,8 GHz.

Transponder wyposażony dodatkowo w wewnętrzne źródło zasilania i nadajnik radiowy jest urządzeniem aktywnym (ang. *active*) i może samodzielnie aktywować wysyłanie danych do czytnika, jeśli znajdzie się w jego zasięgu (który może wynosić nawet do 100 m). Ze względu na bardziej złożoną budowę od transpondera pasywnego, transponder aktywny jest zazwyczaj droższy. Wyróżnia się także transpondery półpasywne (ang. *semi-passive*), które zachowują się jak pasywne, pomimo że mają baterię zasilającą działanie (dzięki której mogą być wykorzystywane do pomiarów temperatury).

Ze względu na możliwości zapisu i odczytu danych wyróżnia się transpondery typu: RO (*Read-Only* – tylko do odczytu), WORM (*Write Once Read Many* – do jednokrotnego zapisu i wielokrotnego odczytu) i RW (*Read/Write* – do wielokrotnego odczytu i zapisu). Dla zwiększenia bezpieczeństwa dane mogą być szyfrowane i zabezpieczane hasłem.

Transpondery mogą być umieszczane w przedmiotach, w ciele ludzi lub zwierząt i mogą przyjmować różną postać: karty plastikowej, etykiety, biletu, breloczka, żetonu, bransoletki czy zegarka. Drukarki RFID umożliwiają samodzielne drukowanie etykiet RFID oraz ich kodowanie (np. zapisanie lub dopisanie danych jawnych lub zaszyfrowanych). W lipcu 2011 roku wrocławska firma PPU COMEX wdrożyła innowacyjną technologię RFID.ON. produkcji etykiet z drukowaną anteną i ukrytym układem RFID, co uniemożliwia oddzielenie go od opakowania produktu [9].

W Polsce, w niektórych bankach (np. PKO BP i PKO SA) wszystkie wydawane karty płatnicze wykorzystują technologię RFID. Karty te działają na zasadzie zbliżeniowej, nie wymagają wprowadzania do czytnika i bez autoryzacji mogą być wykorzystywane do regulowania niewielkich płatności (np. w sklepach, kinach, restauracjach, za bilety komunikacji miejskiej). Wśród około 32 mln wszystkich kart płatniczych, 8 mln to karty zbliżeniowe. Przeprowadzane testy wykazują możliwość nieuprawnionego odczytu danych z karty.

Technologia RFID znajduje szerokie zastosowanie w handlu, logistyce, bankowości, kontroli dostępu do pomieszczeń (nawet w przedszkolach), w elektronicznych legitymacjach studenckich i pracowniczych, paszportach, pilotach samochodowych i garażowych. Mikrochipy RFID umieszczane w dokumentach często zawierają zapisane w sposób elektroniczny dane biometryczne ich właścicieli.

4. Techniki biometryczne

Weryfikacja biometryczna dotyczy w zasadzie organizmów (ludzi, zwierząt), ponieważ oparta jest na porównywaniu cech fizycznych (takich jak wygląd twarzy, linie papilarne palców ręki, tęczówki czy dna oka, układu naczyń krwionośnych ręki itd.) oraz behawioralnych, czyli zachowania (np. sposobu poruszania się, mówienia, pisania na klawiaturze itd.). Przez

porównanie danych cech osobnika z wcześniej zapisanymi w bazie danych weryfikowana jest jego autentyczność. Metody automatycznego porównywania danych biometrycznych są jednak jeszcze niedoskonałe i drogie, stąd nadal nie są powszechnie stosowane. Niedoskonałość biometrii (techniki dokonywania pomiarów) wynika również z niemożności jej stosowania w odniesieniu do wszystkich osób (niektórzy mogą być pozbawieni części ciała niezbędnej do weryfikacji) oraz ze względu na zmienność cech fizycznych i behawioralnych.

Obecnie rozwiązania biometryczne są wykorzystywane do automatycznej kontroli dostępu do pomieszczeń, rejestracji czasu pracy, autoryzacji użytkowników sprzętu (np. komputerowego), a także na lotniskach w USA i w Australii. Wkrótce planowane jest zastosowanie automatycznej kontroli biometrycznej na granicach, z jednoczesnym wykorzystaniem rejestrów policyjnych i celnych. W 2011 roku w Afganistanie wprowadzono Afgański Automatyczny System Identyfikacji Biometrycznej (*Afghan Automated Biometric Identification System* – AABIS) przy Ministerstwie Spraw Wewnętrznych, gromadzący dane biometryczne. W tym celu wyposażono żołnierzy w odpowiednie zestawy sprzętu (laptop, skaner, aparat fotograficzny, urządzenie do pobrania odcisków palców i zeskanowania tęczówek oczu) umożliwiającego pobieranie danych biometrycznych w każdych warunkach.

Na świecie naukowcy w wielu ośrodkach pracują nad opracowaniem wydajnych i bezpiecznych rozwiązań technologicznych elektronicznego uwierzytelniania tożsamości. Przykładem może być projekt TURBINE (*TrUsted Revocable Biometric IdeNtitiEs*) zainicjowany w 2008 roku [13]. Z kolei wdrożony w Polsce w 2000 roku system AFIS (*Automatic Fingerprint Identification System*) – Automatyczny System Identyfikacji Daktyloskopijnej – umożliwia identyfikację osób i zwłok na podstawie zapisów odcisków palca. Baza danych, która jest systematycznie rozbudowywana i uzupełniana, zawiera obecnie ok. 3,4 mln kart daktyloskopijnych i 85 tys. śladów z miejsc przestępstw [1]. Dzięki systemowi możliwe jest wykrywanie sprawców przestępstw nawet po wielu latach.

W Polsce od czerwca 2009 roku wydawane są paszporty biometryczne ze zdjęciem i z elektronicznym zapisem odcisków dwóch palców umieszczonym w chipie RFID wtopionym w okładkę. Od 2016 roku w Polsce będą już tylko tego typu paszporty. Pierwszy paszport elektroniczny na świecie został wydany w Malezji w 1998 roku.

5. Systemy automatycznej identyfikacji – przykłady zastosowań i bezpieczeństwo danych

Systemy identyfikacji i uwierzytelniania nie spełnią swojego zadania, jeśli nie będą współpracowały z dobrze zaprojektowanymi i na bieżąco uaktualnianymi bazami danych, zarządzanymi przez systemy informatyczne zintegrowane z systemami identyfikacji, na

przykład RFID, wspomagając obsługę wymaganych procesów biznesowych, w tym szybkie wyszukiwanie danych i czytelne raportowanie. Budowa takich systemów, ze względu na ich złożoność, jest trudna i czasochłonna. Podczas ich opracowywania trzeba uwzględnić możliwość zmian, na przykład uregulowań prawnych czy zakresu przedsięwzięcia. Wiele projektów ma charakter międzynarodowy więc dochodzą problemy organizacji pracy na odległość zespołu wielokulturowego oraz dostosowywania rozwiązań do norm i przepisów krajowych. Kolejny aspekt to uwzględnianie nowych technologii powiązanych z budowanym systemem. Od obecnych systemów oczekuje się, by umożliwiały pracę zdalną, mobilną. Rozwój oprogramowania nie nadąża za rozwojem sprzętu. Wśród tych wszystkich wymagań niezwykle istotne jest zapewnienie bezpieczeństwa danym i przeprowadzanym transakcjom.

Identyfikacja z wykorzystaniem technologii RFID ma bardzo wiele zalet: cechuje się dużą niezawodnością, jest również łatwa w obsłudze. Liczne przykłady zastosowań tej technologii do automatycznej identyfikacji wskazują na duże korzyści ekonomiczne, organizacyjne czy społeczne, ale niektóre z nich, na przykład regulowanie płatności kartami zbliżeniowymi czy wstrzykiwanie chipów ludziom, nie są całkowicie bezpieczne i mogą naruszać prywatność, dlatego też wywołują obawy lub wręcz oburzenie.

W technologii RFID stosuje się zabezpieczenia na poziomie urządzenia i oprogramowania, między innymi: identyfikatory, szyfrowanie, uwierzytelnianie biometryczne lub kodem PIN, blokowanie przed odczytem, kontrolę poziomu baterii (zbyt niski lub zbyt wysoki poziom sygnalizuje próbę odczytu), klatkę Faradaya (chroniącą przed polem magnetycznym), uszkodzenie anteny (uniemożliwiające odczyt z odległości), polecenie Kill (dezaktywujące nieodwracalnie transponder). Mimo to istnieje zagrożenie nieuprawnionego odczytania danych z transpondera RFID za pomocą odpowiedniego czytnika.

W 2008 roku, w stanie Kalifornia w USA uchwalono prawo, według którego każdy nieuprawniony (czyli bez zgody właściciela) odczyt z urządzenia RFID jest nielegalny. Konieczne jest więc rejestrowanie operacji wykonywanych na danych.

Systemy RFID znajdują zastosowanie w handlu, logistyce czy w bibliotecznych systemach zarządzania (LMS – *Library Management System*) do zabezpieczania książek przed kradzieżą, automatycznej obsługi wypożyczeń i zwrotów oraz do przeprowadzania inwentaryzacji w czasie rzeczywistym.

Nowoczesne rozwiązania informatyczne mogą być wykorzystywane na przykład w systemach do rejestrowania wykroczeń w ruchu drogowym. Umieszczenie w oponie samochodowej chipu RFID umożliwiałoby automatyczne rozpoznawanie pojazdów przekraczających prędkość lub wjeżdżających na skrzyżowanie przy czerwonym świetle. Transpondery RFID są już umieszczane przez firmę Goodyear w oponach aut wyścigowych (od 2006 r.) i ciężarowych (od grudnia 2011 r.) [4]. Od września 2007 roku każdy samochód wyprodu-

kowany w USA musi być wyposażony w system RFID zdalnego kontrolowania ciśnienia w oponach. Na własną prośbę kierowcy w USA mogą otrzymać prawo jazdy z chipem RFID.

W myśl ustawy o bezpieczeństwie imprez masowych z 2009 roku [14], która nałożyła, m.in. na kluby sportowe, obowiązek wdrożenia systemów identyfikacji kibiców, wprowadzono karty identyfikacyjne kibica. W bazie danych systemu identyfikacji są przechowywane dane kibiców i ich zdjęcia. Na terenie obiektów sportowych są rozmieszczane czytniki RFID i kamery. Od stycznia 2012 roku obowiązuje nowelizacja ustawy o bezpieczeństwie imprez masowych [15]. Osobę z zakazem udziału w wybranych imprezach można zobowiązać do przebywania w tym czasie w określonym miejscu (w domu), z założoną bransoletką RFID w zasięgu czytnika, który przekazuje dane do systemu komputerowego. Podobne rozwiązania są stosowane wobec więźniów, osób starszych czy chorych, wymagających nadzoru. Jednak w wielu przypadkach zamiast bransoletek umieszcza się mikrochip RFID w ciele danej osoby (np. osobom z chorobą Alzheimera wszczepiano implanty VeriChip), co jest już sprawą dyskusyjną. Systemy RFID wykorzystuje się w szpitalach do identyfikacji matek i noworodków, w celu zabezpieczenia przez zamianą czy wykradzeniem dziecka [8]. Pojawiła się też kontrowersyjna koncepcja, by mikrochipy wszczepiać dzieciom zaraz po urodzeniu.

Wykorzystanie RFID w medycynie daje ogromne możliwości w połączeniu z oprogramowaniem diagnostycznym. W systemach tych wykorzystywane są zoptymalizowane protokoły zwiększające szybkość odczytu, funkcje przetwarzania wykorzystujące zoptymalizowane algorytmy i dostosowane do potrzeb czytelne raportowanie, ułatwiające podejmowanie decyzji. Bezpieczeństwo gromadzonych danych jest związane z takimi samymi problemami, jak w innych systemach medycznych. Dyskusja toczy się jednak wokół stosowanych praktyk wszczepiania pacjentom chipów RFID (które mogą wywoływać skutki uboczne) oraz na temat wpływu umieszczanych na sprzęcie medycznym etykiet RFID na zdrowie pacjentów i działanie innych urządzeń. Zarządzanie oznakowanymi urządzeniami medycznymi umożliwiają systemy lokalizacji obiektów w czasie rzeczywistym (*Real Time Location System* – RTLS).

W USA od kilku lat trwają prace nad systemem, który z odległości nawet do 25 m, za pomocą wzmocnionych fal terahercowych, będzie automatycznie wykrywać broń u przechodniów [2]. W obliczu takich rozwiązań powstaje pytanie, jakie są jeszcze możliwości systemów identyfikacji oraz jakie dane mogą pozyskiwać. Technologia RFID w połączeniu z systemami lokalizacji GPS umożliwia ciągłe obserwowanie osób i była wykorzystywana przez żołnierzy, którzy ze względów bezpieczeństwa godzili się na wszczepianie mikrochipów. Jednym z takich systemów jest Digital Angel.

Innym niepokojącym projektem jest budowany system o nazwie *Social Radar* (Radar Społeczny), zbierający wszędzie, gdzie tylko to możliwe, dane o obywatelach, w tym biometryczne, medyczne, finansowe, ubezpieczeniowe, dotyczące trybu życia, znajomych, przekonań religijnych i politycznych [10]. System ma wykorzystywać urządzenia pracujące w róż-

nych technologiach (sonary, radary) z wykorzystaniem fal radiowych i podczerwieni oraz różne programy zbierające dane z wszelkich dostępnych źródeł. Uzasadnieniem dla tego przedsięwzięcia jest bezpieczeństwo obywateli, czyli zapobieganie zamachom i konfliktom, ale gromadzenie takich danych jest zagrożeniem dla prywatności.

Standaryzacją w zakresie technologii RFID zajmuje się światowa organizacja GS1, w ramach projektu EPCglobal [3]. Sieć EPCglobal, dzięki połączeniu technologii RFID i sieci globalnej Internet, umożliwia identyfikację obiektów w czasie rzeczywistym. Istotne elementy tej sieci to:

- 96-bitowy kod EPC (*Electronic Product Code*), dla którego opracowano standardy dla pięciu globalnych identyfikatorów EAN/UCC (GTIN, GLN, SSCC, GIAI, GRAI),
- transpondery i czytniki RFID,
- ONS (*Object Name Service*) – metadane o miejscu przechowywania EPC w transponderze (swoisty DNS w odniesieniu do EPC),
- oprogramowanie pośredniczące (*middleware*),
- EPCIS (*EPC Information Service*) – serwer umożliwiający wymianę danych.

Opracowany standard protokołu interfejsu komunikacyjnego (dla pasma 860-960 MHz), o nazwie UHF Class-1 Generation-2, w skrócie oznaczanego Gen 2, ma na celu umożliwienie odczytu tagów przez dowolne czytniki. System GS1 jest zbiorem międzynarodowych standardów i obejmuje: kody kreskowe, elektroniczną komunikację, synchronizację danych i standardy dotyczące technologii RFID. W Polsce jedyną instytucją upoważnioną do przyjmowania członków z naszego kraju do systemu GS1 i nadawania im uprawnień do stosowania kodów kreskowych oraz numerów EPC w systemie GS1 jest Instytut Logistyki i Magazynowania w Poznaniu, który bierze udział w opracowywaniu rozwiązań krajowych oraz w rozwijaniu i dostosowywaniu globalnych standardów. W systemie GS1, z którego korzysta ponad 1 mln przedsiębiorstw ze 150 krajów, wykonuje się ok. 5 mld transakcji dziennie [5].

Większe zastosowanie technologii RFID uzależnione jest od możliwości integracji z innymi, często istniejącymi już, systemami. Funkcjonujące na rynku urządzenia i oprogramowanie różnych producentów w różnych standardach jest nadal barierą w powszechnym wykorzystywaniu. Być może wkrótce, po wprowadzeniu w punktach sprzedaży technologii RFID jednoznacznie identyfikującej klientów i towary oraz wdrożeniu zintegrowanych systemów informatycznych, przy przejściu przez bramkę z czytnikiem RFID nastąpi automatyczne pobranie z konta klienta należnej kwoty za dokonane zakupy.

Od 2010[8] roku miały być wydawane elektroniczne dowody osobiste zaopatrzone w chip RFID z zapisanymi danymi personalnymi oraz podpisem cyfrowym obywatela (i ewentualnie

[8] Termin wydawania dowodów biometrycznych w Polsce pierwotnie planowano na 2010 rok. Ze względu na opóźnienia Sejm w ustawie z dn. 23.07.2010 r. zaproponował przesunięcie terminu na 1 stycznia 2011 roku, ale Senat 6 sierpnia 2010 r. zmienił datę na 1 lipca 2011 r. W nowelizacji ustawy [16] Sejm 9 czerwca 2011 r. przesunął termin na 1 lipca 2013 r.

innymi danymi, np. dotyczącymi grupy krwi czy ubezpieczenia) [12]. Przy okazji zaplanowano przebudowę rejestrów państwowych, tak by dane zbierane przez system, były gromadzone w trzech rejestrach publicznych: PESEL (Powszechny Elektroniczny System Ewidencji Ludności), CRASC (Centralny Rejestr Aktów Stanu Cywilnego, który będzie tworzony w latach 2012 – 2013) oraz RDO (Rejestr Dowodów Osobistych). Bazy danych wykorzystywane w projekcie pl.ID są bardzo duże, na przykład od 2001 roku wydano obywatelom 50 mln dokumentów (dziennie obsługuje się ich ok. 50 tys.) [11]. W styczniu 2012 roku zakończono wdrażanie systemu informatycznego ZMOKU (Zintegrowany Moduł Obsługi Końcowego Użytkownika) we wszystkich gminach w Polsce, wspomagającego ewidencję ludności i wydawanie elektronicznych dowodów osobistych [17]. Podczas realizacji dużych projektów problemem może być zsynchronizowanie zakupu sprzętu z tworzeniem i wdrażaniem oprogramowania, np. zakupiony w ramach projektu pl.ID sprzęt, którego wykorzystanie planowano już od 2010 r., starzeje się i nie jest eksploatowany w okresie gwarancyjnym [6, 12].

Brak bezpieczeństwa danych przechowywanych i przesyłanych, nieuprawnione gromadzenie danych prywatnych i poufnych, korzystanie z nich przez osoby nieupoważnione do celów niezgodnych z przeznaczeniem, to tylko niektóre z wielu obaw związanych z automatyczną identyfikacją z wykorzystaniem technologii RFID i technik biometrycznych.

6. Podsumowanie

Do automatycznej identyfikacji obiektów (ludzi, zwierząt, przedmiotów), polegającej na automatycznym pozyskiwaniu danych i przekazywaniu ich do odpowiednich systemów w celu ich zidentyfikowania, wykorzystywane są różne technologie. Powszechne dotychczas kody kreskowe zastępowane są nowocześniejszymi systemami identyfikacji radiowej RFID, które opierają swoje działanie na czterech komponentach: transponderach, czytnikach, bazach danych i oprogramowaniu. Zastosowanie technologii RFID jest jeszcze niewielkie w stosunku do możliwości, stąd można oczekiwać, że w najbliższym czasie zainteresowanie nią (w połączeniu z metodami biometrycznymi) bardzo wzrośnie. W tym celu konieczne jest jednak opracowanie i przestrzeganie standardów oraz budowa profesjonalnych, odpowiednio zabezpieczonych, systemów informatycznych i centralnych rejestrów danych. Istotna jest również cena urządzeń, gdyż do masowego zastosowania potrzebne są ogromne ilości transponderów i czytników (kompatybilnych, a zarazem niezakłócających nawzajem swojej pracy). Istotnym zadaniem jest przekonanie obywateli do tych nowych technologii, gdyż fakt, że ułatwiają i przyspieszają pracę jest zarówno zaletą, jak i wadą, ponieważ pracownicy niepokoją się o utratę zatrudnienia.

Prace nad automatyczną identyfikacją są wielokierunkowe. Wiele zastosowań technologii RFID wzbudza kontrowersje i istnieją uzasadnione obawy, że wraz z wprowadzeniem nowych rozwiązań na szeroką skalę, bezpowrotnie zostanie utracona prywatność obywateli oraz kontrola nad gromadzeniem ich danych. Bez wiedzy zainteresowanych będą z pewnością zbierane i przetwarzane dane biometryczne oraz dotyczące trybu życia, zakupów, kręgu znajomych, wymiany korespondencji, przemieszczania się, przejazdów komunikacyjnych, udziału w imprezach masowych, pobytu w ośrodkach rekreacyjno-sportowych, płatnościach finansowych itd. Wiele danych gromadzonych jest już teraz za pomocą powszechnie wykorzystywanych urządzeń elektronicznych.

Automatyczna identyfikacja wykorzystująca urządzenia miniaturowych rozmiarów i niewidoczne fale radiowe umożliwia niezauważalne zbieranie dowolnych danych. Nie ma pewności, czy za jakiś czas zamontowane czytniki nie będą automatycznie przechwytywały informacje o stanie zdrowia lub zawartości toreb, lub odczytywały dane z dokumentów, urządzeń elektronicznych i kart płatniczych. Technologia ta może być też wykorzystywana przez przestępców w różnych celach. Prowadzone kierunki prac badawczych i wdrożeniowych, związanych z automatyczną identyfikacją, wzbudzają ogromny niepokój o nieograniczone i nieprzewidywalne do końca możliwości jej wykorzystywania.

BIBLIOGRAFIA

1. AFIS, www.clk.policja.pl/portal/clk/504/65734/Zespol_AFIS.html.
2. Baker A.: Police Working on Technology to Detect Concealed Guns. 17 January 2012, www.cityroom.blogs.nytimes.com/2012/01/17/.
3. EPCglobal, www.gs1.org/epcglobal.
4. Goodyear Markets First Microchipped Truck Tires, www.goodyear.eu.
5. GS1 Polska, www.gs1pl.org.
6. Jadczak A.: Budowa systemu PL.ID i nowe dowody odsunięte w czasie. Computerworld, 08.04.2011, computerworld.pl/news/369069.
7. Kody kreskowe – czytniki kodów kreskowych. Strona AutoID Polska S.A., www.autoid-.pl.
8. Makarenko V.: W szpitalu: mama, dziecko i chip. 23.04.2009, www.gazeta.pl.
9. Nowy produkt RFID.ON., 04.08.2011, www.comex.net.pl.
10. Shachtman N.: Air Force's Top Brain Wants a „Social Radar" to „See Into Hearts and Minds". 19.01.2012, www.wired.com/dangerroom/2012/01/social-radar-sees-minds.
11. Statystyki Centrum Personalizacji Dokumentów MSW, www.cpd.msw.gov.pl/o_nas.
12. Strona projektu pl.ID, www.cpi.mswia.gov.pl.
13. TURBINE, www.turbine-project.eu.

14. Ustawa o bezpieczeństwie imprez masowych (Dz. U. Nr 62 poz. 504) z 20 marca 2009 r.
15. Ustawa z dnia 31 sierpnia 2011 r. o zmianie ustawy o bezpieczeństwie imprez masowych oraz niektórych innych ustaw, http://isap.sejm.gov.pl/DetailsServlet? id=WDU2011-2171280.
16. Ustawa z dnia 9 czerwca 2011 r. o zmianie ustawy o dowodach osobistych i ustawy o ewidencji ludności, Dz.U. 2011 nr 133 poz. 768.
17. ZMOKU, www.mojdowod.pl.

Wpłynęło do Redakcji 24 stycznia 2012 r.

Abstract

The interest in automatic object identification with the use of bar codes, RFID technology and biometric methods is now quite significant and keeps growing. Deployment of these technologies and methods brings numerous advantages: lower costs of running a business, quicker and easier customer service, theft and forgery prevention, possibility for identification of moving objects and objects in inaccessible areas. This, however, requires development of relevant standards, legal regulations, and IT systems (databases with software). This paper presents issues related to the development of automatic object identification systems in the context of new applications, data processing and security of stored data.

Adresy

Zygmunt MAZUR: Politechnika Wrocławska, Instytut Informatyki, Wyb. Wyspiańskiego 27, 50-370 Wrocław, Polska, zygmunt.mazur@pwr.wroc.pl.
Hanna MAZUR: Politechnika Wrocławska, Instytut Informatyki, Wyb. Wyspiańskiego 27, 50-370 Wrocław, Polska, hanna.mazur@pwr.wroc.pl.