Ekonomiczne Problemy Usług nr 1/2017 (126), t. 1

ISSN: 1896-382X | www.wnus.edu.pl/epu
DOI: 10.18276/epu.2017.126/1-25 | strony: 243–255

Jarosław Napiórkowski, Jerzy Stanik
Wojskowa Akademia Techniczna
Wydział Cybernetyki, Instytut Systemów Informatycznych
e-mail: jaroslaw.napiorkowski@wat.edu.pl, jerzy.stanik@wat.edu.pl

Zastosowanie technologii RFID do zarządzania obiegiem dokumentów niejawnych

Kody JEL: F52, L32, O14, O33
Słowa kluczowe: bezpieczeństwo informacji, informacje niejawne, nowe technologie, proces biznesowy, RFID
Streszczenie. W artykule autorzy podejmują tematykę zastosowania technologii RFID w zakresie wytwarzania, obiegu i wykorzystywania dokumentów niejawnych. Przybliżono także tematykę samej technologii RFID oraz podejścia do jej wdrażania przy różnego typu zastosowaniach ze szczególnym uwzględnieniem zastosowania do budowy kancelarii tajnej. Przedstawione są mocno nasycone technologią RFID modele procesów biznesowych realizowanych w kancelarii. Zaprezentowano prawne możliwości stosowania technologii RFID do zarządzania obiegiem dokumentów niejawnych.

Wprowadzenie

Podstawą prawną ochrony informacji niejawnych w Polsce jest Ustawa z 5 sierpnia 2010 roku o ochronie informacji niejawnych (Dz.U. 2010, nr 182, poz. 1228) wraz z aktami wykonawczymi. W myśl ustawy informacją niejawną jest każda informacja, której nieuprawnione ujawnienie spowodowałoby lub mogłoby spowodować szkody dla Rzeczpospolitej Polskiej. Informacje te podlegają ochronie już w trakcie ich opracowywania, natomiast dla samej ich ochrony nie ma znaczenia forma, sposób wyrażenia oraz sposób utrwalenia.

Najpopularniejszą obecnie formą utrwalenia informacji niejawnej jest dokument – za taki uważana jest każda utrwalona informacja niejawna, w szczególności na piśmie, mikrofilmach, negatywach i fotografiach, nośnikach do zapisów informacji w postaci cyfrowej (nośnikach informatycznych) i na taśmach elektromagnetycznych, także

w formie mapy, wykresu, rysunku, obrazu, grafiki, fotografii, broszury, książki, kopii, odpisu, wypisu, wyciągu i tłumaczenia dokumentu, zbędnego lub wadliwego wydruku, odbitki, kliszy, matrycy i dysku optycznego, kalki, taśmy atramentowej, jak również informacja niejawna utrwalona na elektronicznych nośnikach danych (Adamczyk, 2015).

Szeroki zakresu regulacji wprowadzonych przez ustawodawcę nie wskazuje na istnienie jakichkolwiek predefiniowanych procesów związanych z ochroną informacji niejawnych. Ustawa wraz z aktami wykonawczymi stanowi jedynie podstawę do budowy dostosowanego do potrzeb danej jednostki organizacyjnej systemu ochrony informacji niejawnych, a kierownik jednostki organizacyjnej decyduje o identyfikacji i sposobie implementacji tych procesów.

Dobre praktyki w zakresie inżynierii systemów, modelowania procesów biznesowych, dokumenty normatywne, wytyczne (Napiórkowski, Stanik, 2015) oraz regulacje prawne, wykorzystujące możliwości jakie daje współczesny rozwój technologii dają możliwość adaptacji dobrze znanych rozwiązań do zupełnie nowych celów.

Wykorzystanie technologii RFID (*Radio-Frequency IDentification*) przy budowie systemu zabezpieczającego ewidencjonowanie, monitorującego nadzór nad dostępem do materiałów niejawnych oraz ich obiegu może być dobrym przykładem takiej innowacyjnej adaptacji dobrze znanej technologii.

Celem niniejszego artykułu jest zaprezentowanie podejścia do wdrażania systemów wspieranych technologią RFID oraz jej praktycznego zastosowania w zarządzaniu obiegiem dokumentów niejawnych. Zasygnalizowano również konieczność dostosowania obecnych, krajowych przepisów ochrony informacji niejawnych pod kątem stosowania w tym obszarze nowych rozwiązań i innowacyjnych narzędzi – elementów budujących przewagę konkurencyjną przedsiębiorstw i organizacji w dobie gospodarki opartej na wiedzy.

1. Opis systemu RFID

Technologia RFID jest sposobem identyfikacji obiektów (przedmiotów lub osób) za pomocą fal radiowych. Identyfikacja ta jest możliwa przy użyciu unikatowych numerów, które identyfikują obiekty. Sama identyfikacja częstotliwości radiowej to technologia znana już od pewnego czasu. Już w czasie II wojny światowej w celu identyfikacji i uwierzytelnienia własnych samolotów, wykorzystywano identyfikację w systemie zwanym „identyfikacją przyjaciel czy wróg" (*Identification Friend or Foe, IFF*) i jest wciąż używane dzisiaj do tych samych celów (Griffin, 2005).

Do poprawnego działania systemu wymagany jest interrogator oraz transponder. Interrogator wysyła zapytanie do transpondera, po czym transponder odpowiada na zapytanie w określony sposób. System ten, który początkowo używany był wyłącznie do rozróżnienia między maszynami własnymi oraz wrogimi, ewoluował z czasem przybierając ostatecznie postać IFF, używanego w różnych trybach, w tym także do odróż-

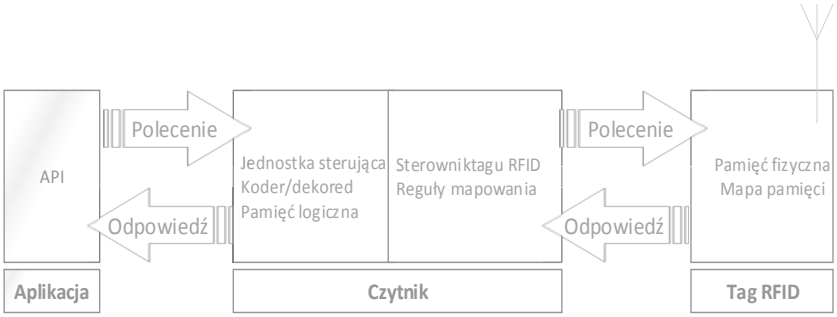
niania cywilnych i zagranicznych statków powietrznych. Istnieją dwa główne tryby pracy systemu:

- SIF (*Selective Identification Facility*) – tryb jawny,
- SM (*Secure Mode*) – tryb tajny, uruchamiany w przypadku wojny lub w celu sprawdzenia jego działania.

Obecnie technologia RFID to jeden z dzisiaj najszybciej rozwijających się segmentów automatycznego zbierania danych identyfikujących (*Automatic Identification Data Collection* – AIDC), w którym w przeciwieństwie do powszechnie stosowanych dzisiaj kodów kreskowych informacje mogą być odczytywane automatycznie.

Typowy system RFID składa się z trzech głównych komponentów:

- tag RFID (etykieta RFID, transponder), który jest umieszczony na obiekcie podlegającym, jest nośnikiem danych w systemie RFID,
- czytnik RFID (interrogator, transceiver), który ma możliwość zarówno odczytu, jak i zapisu danych na transponderze,
- podsystem przetwarzania danych (aplikacja), który wykorzystuje dane uzyskane z urządzenia nadawczo-odbiorczego w jakiś użyteczny sposób.



Rysunek 1. Elementy systemu RFID

Źródło: opracowanie własne na podst. Griffin (2005).

Obecnie najpopularniejsze zastosowanie technologii RFID to przede wszystkim obszar logistyki (automatyczne zliczanie towaru przy przejazdach przez punkty kontrolne, eliminacja pomyłek przy załadunku), transportu (systemy poboru opłat, kontrola ilości i zawartości załadunku i rozładunku), ale również bezpieczeństwa. Zastosowanie technologii RFID w bezpieczeństwie to najczęściej zastosowania związane z ochroną antykradzieżową czy też system kontroli dostępu. Te ostatnie służą do elektronicznej identyfikacji użytkownika, zarządzania i kontroli obecności użytkowników w strefach systemu czy też bieżącego dostępu do zdarzeń występujących w systemie. Coraz częściej technologia RFID znajduje zastosowanie w bibliotekach podczas bezosobowej obsłudze zwrotu książek. Właśnie oszczędność czasu, automatyzacja procesów, szybkość i dokładność w dostępne do informacji oraz eliminowanie błędów to główne cele stosowania technologii RFID.

2. Wdrożenie systemu RFID

Samo wdrożenie technologii RFID nie jest przedsięwzięciem skomplikowanym. Wdrażając tego typu rozwiązania, należy jednak brać pod uwagę związane z tym ograniczenia zarówno biznesowe, jak i technologiczne. Przykładem tych pierwszych może być wysoki początkowy koszt wdrożenia rozwiązania czy też konieczność współdzielenie danych z partnerami w łańcuchu dostaw. Ewentualne problemy związane z technologią to kwestie środowiskowe (temperatura pracy, wilgotność, rodzaje podłoża i użytych materiałów), ale też poprawność odczytu znaczników czy bezpieczeństwo danych na tagach RFID i czytnikach oraz znaczne ilości rejestrowanych w systemie danych. Decydując się na użycie tej technologii, nie należy również zapominać o dość łatwym blokowaniu sygnału RFID. To co w przypadku celowego blokowania sygnału (np. celowe stosowanie specjalnego zabezpieczania kart bankowych) jest zjawiskiem pożądanym, w przypadku zastosowań logistycznych chodzi przede wszystkim o niezakłóconą komunikację pomiędzy czytnikiem a tagami RFID.

Niezależnie od obszaru zastosowań projektując system RFID, tak jak w przypadku każdego innego system, należy zdefiniować wymagania systemu oraz zaprojektować jego architekturę (Napiórkowski, Waszkowski, 2015). Uzyskanie na etapie analizy odpowiedzi na poniższe pytania może być pomocne, aby właściwie zaprojektować system RFID:

- dlaczego wdrażamy system RFID,
- czy używane będą tagi wielokrotnego użytku czy jednorazowe,
- jakie jest wymaganie dotyczące rodzaju używanych tagów (R/O[1], R/W[2], WORM[3]),
- jaka jest maksymalna ilość danych, które mają być zapisane w tagu,
- jaki format danych będzie użyty,
- gdzie i w jaki sposób tagi będą stosowane,
- co należy zrobić jeśli tag został odczytany,
- co należy zrobić jeśli tag nie został odczytany,
- jaka ma być strefa odczytu czytnika,
- jak dużo tagów będzie jednocześnie odczytywanych lub zapisywanych przez czytnik,
- jaki jest ustawienie tagów i odległości miedzy nimi,
- jaka kontrola i korekcja błędów będzie wymagana,
- jaka jest odległość pomiędzy antenami czytników,

[1] Tagi typu R/O (*Read/Only*) – dane zapisane w procesie produkcji (tylko numer seryjny identyfikatora), nie ma możliwości zapisu dodatkowych danych jak również zmiany wartości samego numeru seryjnego.

[2] Tagi typu R/W (*Read/Write*) – wielokrotny zapis danych, bez możliwości zmiany numeru seryjnego.

[3] Tagi typu WORM (*Write Once Read Many Times*) – jednorazowy zapis danych, bez możliwości zmiany numeru seryjnego.

- czy potrzebujemy chronić dane,
- jaka jest odległość pomiędzy antena a czytnikiem,
- jakie są wymagania dotyczące mobilności elementów systemu RFID,
- jaka jest odległość tagów i anten do powierzchni metalowych, płynów itp.,
- jakie warunki środowiskowe takie jak temperatura i wilgotność panują w otoczeniu systemu,
- co wiemy o narażeniu na chemikalia, promieniowanie UV, promieniowanie rentgenowskie, naprężenia mechaniczne, zapylenie,
- jaki jest średni koszt taga,
- jak wdrożenie systemu RFID wpłynie na wynik (m.in. finansowy, poprawę bezpieczeństwa).

Jak widać projektując system należy zwrócić uwagę na nie tylko na to czy wdrożenie takiego rozwiązania usprawni realizowane w organizacji procesy, ale również na odpowiedni dobór elementów systemu oraz panujące w jego otoczeniu warunki środowiskowe.

3. Budowa modelu kancelarii niejawnej

Znajomość samej technologii RFID, regulacji prawnych oraz wymagań stawianych przed kancelarią działającą przy wsparciu technologii RFID pozwoliła na zbudowanie koncepcji zarówno modelu fizycznego, jak i logicznego działania kancelarii niejawnej. Na podstawie przeglądu istniejących rozwiązań technicznych w obszarze technologii RFID opracowano (Marciniak, 2015) opis wybranych cech technologii RFID, co dało podstawę do podjęcia decyzji o zastosowaniu tych rozwiązań dla ochrony dokumentów.

Podstawą do zbudowania modelu kancelarii dla dokumentów zawierających informacje niejawne były zatem wymagania zapewniające (Adamczyk, Kiryk, Napiórkowski, Walczak, 2016):

- bezpieczne przechowywanie istniejących dokumentów,
- bezpieczny obieg dokumentów wraz z realizacją postulatu pełnej rozliczalności zarówno dla dokumentu jak i użytkownika,
- bezpieczne warunki do pracy z dokumentami,
- bezpieczne warunki do opracowywania nowych dokumentów.

Budowę modelu kancelarii obejmującego podstawowe kryteria jej organizacji, które należało uwzględnić oparto przede wszystkim na analizie wymagań prawnych. W trakcie ich analizy stwierdzono brak jakichkolwiek uregulowań prawnych lub normatywnych, z których można by skorzystać chcąc zastosować technologię RFID jako element ochrony dokumentów zawierających informacje niejawne. W budowie modelu wykorzystano następujące regulacje:

- Rozporządzenie Prezesa Rady Ministrów z 7 grudnia 2011 roku w sprawie nadawania, przyjmowania, przewożenia, wydawania i ochrony materiałów zawierających informacje niejawne (Dz.U. 2011, nr 271, poz. 1603),
- Rozporządzenie Rady Ministrów z 7 grudnia 2011 roku w sprawie organizacji i funkcjonowania kancelarii tajnych oraz sposobu i trybu przetwarzania informacji niejawnych (Dz.U. 2011, nr 276, poz. 1631),
- Rozporządzenie Prezesa Rady Ministrów z 22 grudnia 2011 roku w sprawie sposobu oznaczania materiałów i umieszczania na nich klauzul tajności (Dz.U. 2011, nr 288, poz. 1692),
- Rozporządzenie Rady Ministrów z 29 maja 2012 roku w sprawie środków bezpieczeństwa fizycznego stosowanych do zabezpieczania informacji niejawnych (Dz.U. 2012, poz. 683),
- Rozporządzenie Rady Ministrów z 21 grudnia 2012 roku zmieniające rozporządzenie w sprawie organizacji i funkcjonowania kancelarii tajnych oraz sposobu i trybu przetwarzania informacji niejawnych (Dz.U. 2013, nr 0, poz. 11).

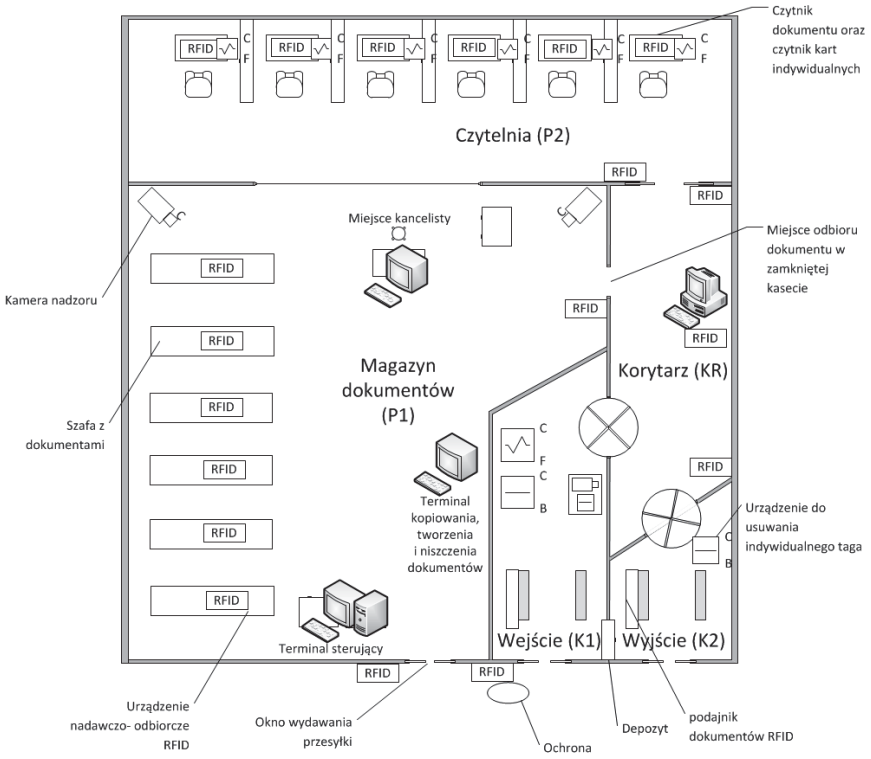
Analiza powyższych regulacji pozwoliła na wyszczególnienie ról, zasobów i procesów z jakim zbudowano model kancelarii. Wyróżniono następujące role: Kancelista, Ochroniarz, Użytkownik, Konwojent Poczty Specjalnej.

Dalsza analiza wskazała, że w przypadku zastosowania technologii RFID spełnienie wymagań prawnych będzie możliwe przy dysponowaniu poniższymi zasobami, takimi jak urządzenia i elementy niezbędne do działania kancelarii niejawnej (Stanik, Kiedrowicz, 2015; Adamczyk, Kiryk, Napiórkowski, Walczak, 2016):

- szafy na materiały niejawne zawierające czytniki RFID,
- szafki na rzeczy,
- stanowisko kancelisty z czytnikiem indywidualnego RFID i korytkiem do sczytywania tagów materiałów niejawnych,
- terminal z czytnikiem RFID,
- bramka wykrywająca metale wraz z torem na materiały niejawne zawierającym skaner rentgenowski i czytnik RFID (tor ten jest przeznaczony na pojemnik z materiałami niejawnymi oznaczonymi tagami RFID),
- urządzenie do identyfikacji biometrycznej,
- czytnik RFID przed drzwiami wejściowymi i wyjściowymi,
- drukarka sieciowa u kancelisty,
- kserokopiarka u kancelisty,
- okienko na specjalną pocztę,
- stanowisko w czytelni z korytkiem na dokumenty oznaczone tagami RFID, z czytnikiem indywidualnego taga RFID oraz z terminalem lub komputerem,
- urządzenie do zakładania jednorazowego taga,
- urządzenie do ściągania jednorazowego taga,

– urządzenia do niszczenia materiałów niejawnych (np. niszczarka do dokumentów papierowych, niszczarka do płyt CD/DVD, demagnetyzer do dysków HDD).

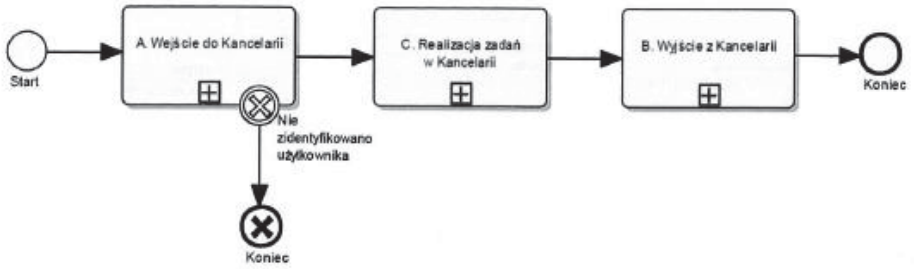
Pozwoliło to na zbudowanie koncepcji (Kiedrowicz, 2015) wzorcowej kancelarii, która zapewni wymaganą, regulacjami prawnymi, ochronę dokumentów niejawnych przechowywanych w kancelarii stosującej do ich ochrony technologie RFID.



Rysunek 2. Schemat kancelarii tajnej wraz z czytelnią dokumentów

Źródło: Adamczyk i in. (2015).

Poza wyspecyfikowaniem ról i elementów systemu opracowano (Adamczyk i in., 2015) opis procesów realizowanych w kancelarii. Jako proces ogólny wskazano obsługę petenta.



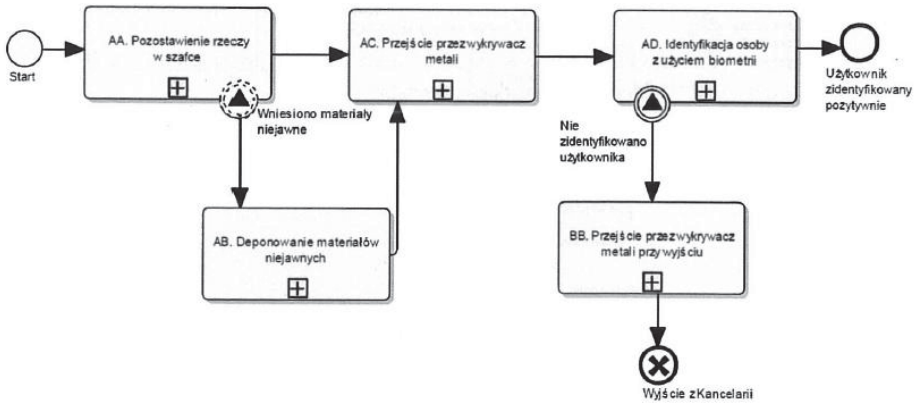
Rysunek 3. Proces ogólny pracy kancelarii: obsługa petenta

Źródło: Adamczyk i in. (2015).

Powyższy diagram opisuje podprocesy:

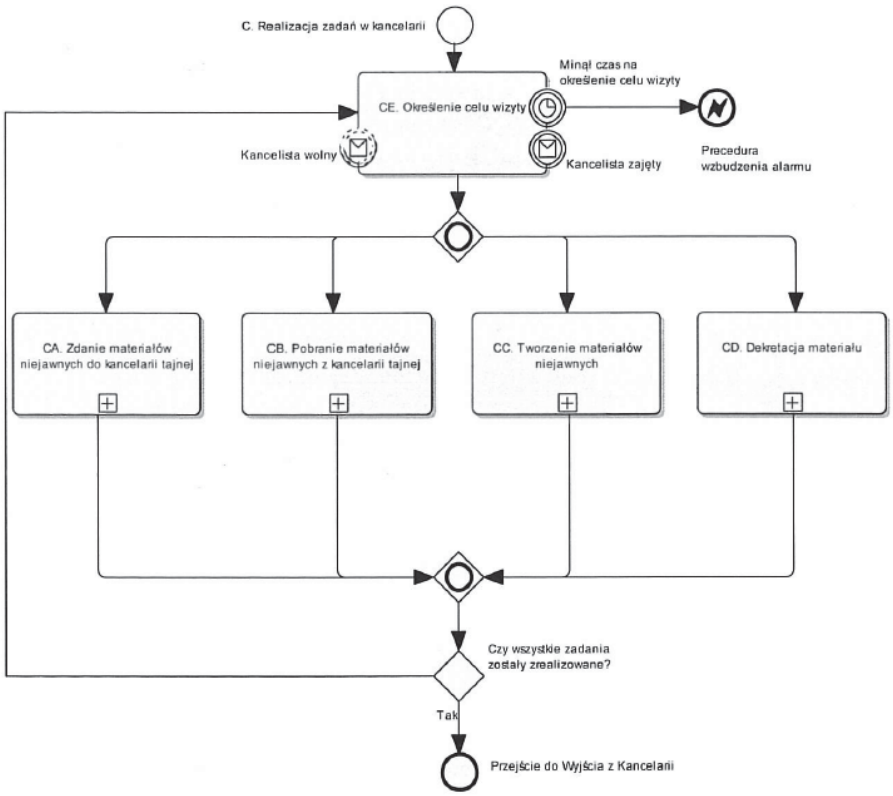
- wejścia do kancelarii wraz ze szczegółowym opisem procedur, które muszą zostać zrealizowane, aby otrzymać dostęp do kancelarii,
- realizacji zadań w kancelarii wraz ze szczegółowym opisem procedur, które są realizowane podczas pobytu w kancelarii,
- wyjścia do kancelarii wraz ze szczegółowym opisem procedur, które muszą zostać zrealizowane, aby opuścić kancelarię.

W dalszej części (rys. 4, 5, 6) przedstawiono rozwinięcie podprocesów.



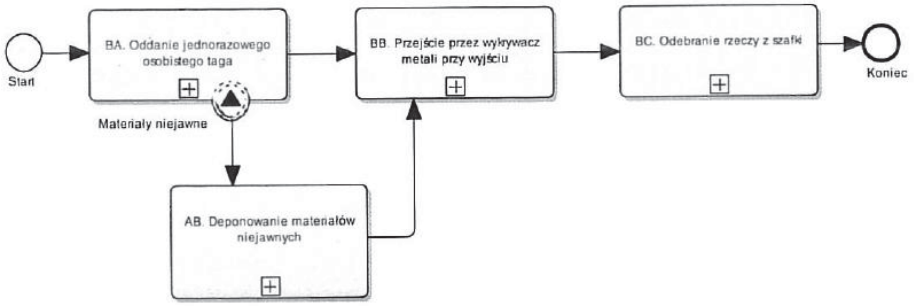
Rysunek 4. Diagram procesu: wejście do kancelarii niejawnej

Źródło: Adamczyk i in. (2015).



Rysunek 5. Diagram procesu: realizacja zadań w kancelarii

Źródło: Adamczyk i in. (2015).



Rysunek 6. Diagram procesu: wyjście do kancelarii niejawnej

Źródło: Adamczyk i in. (2015).

Wiele zadań realizowanych w trakcie całego procesu wiąże się z wykorzystaniem technologii RFID. Liczbę elementów systemu wykorzystujących technologie RFID

widać na schemacie kancelarii tajnej wraz z czytelnią dokumentów (rys. 2). Są to dla przykładu procesy:

- AB – deponowanie materiałów niejawnych (rys. 4) – petent deponując materiały niejawne oznaczone tagami RFID, wkłada je do dedykowanego pojemnika i odkłada pojemnik na taśmę transportującą,
- AC – przejście przez wykrywacz metali przy wejściu (rys. 4) – petent pojemnik z materiałami niejawnymi oznaczonymi tagami RFID umieszcza na torze skanowania,
- AD – identyfikacja osoby przy użyciu biometrii (rys. 4) –petentowi zakładany jest jednorazowy tag RFID a użytkownik otwiera drzwi przy jego użyciu.

Na szczególną uwagę zasługuje bardziej dokładny opis zadań w trakcie realizacji procesu CA – zdanie materiałów niejawnych do kancelarii tajnej (rys. 5). W trakcie tego procesu weryfikowana jest zarówno sama tożsamość petenta (Zadanie CA.1), jak i zadania CA.3 (weryfikacja kompletności i skanowanie materiałów niejawnych oznaczonych tagami RFID) i CA.6 (weryfikacja i skanowanie materiałów niejawnych umieszczonych w szafie). Wszystkie powyższe zadania (CA.1, CA.3 i CA.6) w przypadku stwierdzenia rozbieżności ze stanem oczekiwanym wzbudzają alarm.

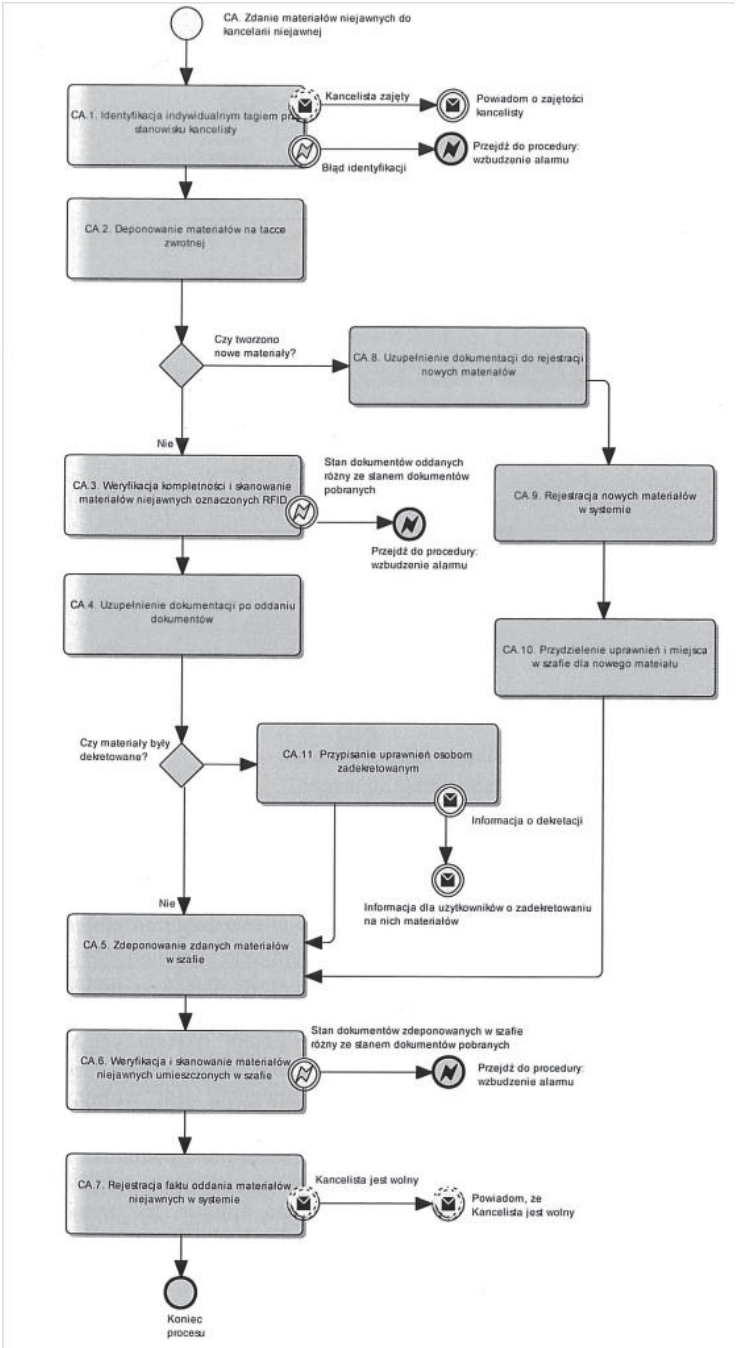
Istotną z punktu widzenia kontroli obiegu dokumentów niejawnych są stosowanie w prezentowanym systemie inteligentnych szaf na dokumenty (rys. 2), które (zadanie CA.6) w połączeniu z dedykowanym systemem, rejestrują i zapisują wszystkie zmiany zawartości szafy, są wstanie sporządzić automatyczną inwentaryzację.

Podsumowanie

Systemy RFID są powszechnie wykorzystywane w logistyce i gospodarce materiałowej. Coraz powszechniej wykorzystywane są również przez urzędy, archiwa, sądy i biblioteki, które korzystają z tej technologii przy kontroli dostępu oraz lokalizacji dokumentacji czy akt. Policja czy wojsko używają tej technologii do ewidencji sprzętu techniki specjalnej. Niewątpliwą zaletą stosowania tej klasy rozwiązań jest szybkość, jakość i niezawodność, które mają zasadnicze znaczenie dla jej masowego wykorzystywania w zakresie wytwarzania, obiegu i wykorzystywania dokumentów wrażliwych.

Systemy RFID wydają się zatem dobrym uzupełnieniem technologicznych luk w obecnych systemach ochrony informacji niejawnych oraz mogą stanowić podstawę do budowy systemów automatycznego nadzoru nad materiałami, będącymi nośnikami lub swoim bytem stanowiącymi informację, którą należy w szczególny sposób chronić.

Kwestią czasu jest więc chyba, w ramach realizacji ważnych zadań publicznych, dostosowanie przepisów ochrony informacji niejawnych do zmian zachodzących w środowisku nowych technologii.



Rysunek 7. Diagram procesu: zdanie materiałów niejawnych do kancelarii tajnej

Źródło: Adamczyk i in. (2015).

Publikacja zrealizowana w ramach projektu naukowo-badawczego pt. „Elektroniczny system zarządzania cyklem życia dokumentów o różnych poziomach wrażliwości", nr umowy z Narodowym Centrum Badań i Rozwoju: DOBR-BIO4/006/13143/2013.

Bibliografia

Adamczyk, P. (2015). Prawne aspekty ochrony informacji niejawnych z uwzględnieniem technik znakowania RFID. W: M. Kiedrowicz (red.), *Zarządzanie informacjami wrażliwymi. Wybrane aspekty organizacyjne, prawne i techniczne ochrony informacji niejawnych*. Warszawa: Wojskowa Akademia Techniczna.

Adamczyk, P., Kiryk, G., Napiórkowski, J, Walczak, A. (2016). Sieciowy model systemu bezpieczeństwa. W: M. Kiedrowicz (red.), *Zarządzanie informacjami wrażliwymi. Bezpieczeństwo dokumentów, wykorzystanie technologii RFID.* Warszawa: Wojskowa Akademia Techniczna.

Adamczyk, P., Bieniek, B., Derski, T., Holeczko, J., Napiórkowski, J., Paczkowski, M., Piotrowsk,i P., Walczak, A. (2015). Model kancelarii niejawnej w wykorzystaniem technologiiRFID. W: M. Kiedrowicz (red.), *Zarządzanie informacjami wrażliwymi. Wybrane aspekty organizacyjne, prawne i techniczne ochrony informacji niejawnych*. Warszawa: Wojskowa Akademia Techniczna.

Griffin, S., Williams, C. (2005). *RFID Futures in Western Europe. White Paper*. Juniper Research. Pobrano z: http://www.logisticsit.com.

Lehpamer, H. (2008). *RFID Design Principles*. Norwood: ARTECH HOUSE, INC.

Kiedrowicz, M. (red.). (2015). *Zarządzanie informacjami wrażliwymi. Wybrane aspekty organizacyjne, prawne i techniczne ochrony informacji niejawnych*. Warszawa: Wojskowa Akademia Techniczna.

Kiedrowicz, M. (red.). (2016). *Zarządzanie informacjami wrażliwymi. Bezpieczeństwo dokumentów, wykorzystanie technologii RFID.* Warszawa: Wojskowa Akademia Techniczna.

Marciniak, P. (2015). Przegląd wybranych cech technologii RFID. W: M. Kiedrowicz (red.), *Zarządzanie informacjami wrażliwymi. Wybrane aspekty organizacyjne, prawne i techniczne ochrony informacji niejawnych.* Warszawa: Wojskowa Akademia Techniczna.

Napiórkowski, J., Stanik, J. (2015). *A security subsystem design for a secret registry using RFID solutions*. W: B.F. Kubiak, J. Maślankowski (red.), *Information Management in Practice* (s. 211–229). Sopot: Faculty of Management, University.

Napiórkowski, J., Waszkowski, R. (2015). *System architecture for the classified document lifecycle management*. W: B.F. Kubiak, J. Maślankowski (red.), *Information Management in Practice* (s. 335–345). Sopot: Faculty of Management, University.

Rozporządzenie Prezesa Rady Ministrów z dnia 7 grudnia 2011 r. w sprawie nadawania, przyjmowania, przewożenia, wydawania i ochrony materiałów zawierających informacje niejawne (Dz.U. 2011, nr 271, poz. 1603).

Rozporządzenie Rady Ministrów z dnia 7 grudnia 2011 r. w sprawie organizacji i funkcjonowania kancelarii tajnych oraz sposobu i trybu przetwarzania informacji niejawnych (Dz.U. 2011, nr 276, poz. 1631).

Rozporządzenie Prezesa Rady Ministrów z dnia 22 grudnia 2011 r. w sprawie sposobu oznaczania materiałów i umieszczania na nich klauzul tajności (Dz.U. 2011, nr 288, poz. 1692).

Rozporządzenie Rady Ministrów z dnia 29 maja 2012 r. w sprawie środków bezpieczeństwa fizycznego stosowanych do zabezpieczania informacji niejawnych (Dz.U. 2012, poz. 683).

Rozporządzenie Rady Ministrów z dnia 21 grudnia 2012 r. zmieniające rozporządzenie w sprawie organizacji i funkcjonowania kancelarii tajnych oraz sposobu i trybu przetwarzania informacji niejawnych (Dz.U. 2013, nr 0, poz. 11).

Stanik, J., Kiedrowicz, M. (2015). *Selected aspects of risk management in respect of security of the document lifecycle management system with multiple levels of sensitivity*. W: B.F. Kubiak, J. Maślankowski (red.), *Information Management in Practice* (s. 231–251). Sopot: Faculty of Management, University.

Ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz.U. 2010, nr 182, poz. 1228).

THE USE OF RFID TECHNOLOGY TO MANAGE THE FLOW OF CLASSIFIED DOCUMENTS

Keywords: classified information, new technology, information security, business process, RFID

Summary. The authors take the subject of the use of RFID technology in generation, flow and use of classified documents. The article describes RFID technology, his implementation of the various types of applications with special focus on building secret registry. The article presented business processes models implemented in secret registry and their large use of RFID technology. Presented are legal possibilities to use RFID technology to manage the flow of classified documents.

Translated by Jarosław Napiórkowski

Cytowanie

Napiórkowski, J., Stanik, J. (2017). Zastosowanie technologii RFID do zarządzania obiegiem dokumentów niejawnych. *Ekonomiczne Problemy Usług*, 1 (126/1), 243–255. DOI: 10.18276/epu.2017.126/1-25.