Maciej Kiedrowicz[1], Jarosław Koszela[2]

Model kancelarii przetwarzającej dokumenty wrażliwe z wykorzystaniem technologii RFID

1. Wstęp

Dokumenty o różnych poziomach wrażliwości obejmują dokumenty, które wymagają szczególnego podejścia do zarządzania nimi. Mogą one zawierać zarówno informacje niejawne, jak i te, które powinny być szczególnie chronione ze względu na inne aspekty (np. dokumenty bankowe). Obsługa tego rodzaju dokumentów odbywa się zazwyczaj w dostosowanych do tego celu pomieszczeniach – stąd też pojęcia kancelarii niejawnej lub kancelarii RFID[3], wykorzystywane w dalszej części opracowania. Podstawowym założeniem, które przyjęto, jest możliwość wykorzystania technologii RFID[4] do znakowania dokumentów i zarządzania nimi przy uwzględnieniu jej możliwości i aktualnie obowiązującego stanu prawnego dotyczącego przetwarzania dokumentów wrażliwych. Podstawowym celem tego artykułu jest przedstawienie głównych aspektów organizacji i funkcjonowania kancelarii przetwarzających dokumenty oraz materiały niejawne zgodnie z aktualnie obowiązującym stanem prawnym w Polsce, a także modelu kancelarii, w której podstawowa funkcjonalność jest wspomagana przez zastosowanie dedykowanych systemów teleinformatycznych i technologii RFID.

---

[1] Wojskowa Akademia Techniczna w Warszawie, Wydział Cybernetyki.
[2] Wojskowa Akademia Techniczna w Warszawie, Wydział Cybernetyki.

[3] RFID (ang. *radio-frequency identification*) – technika, która wykorzystuje fale radiowe do przesyłania danych oraz zasilania elektronicznego układu (etykieta RFID) stanowiącego etykietę obiektu przez czytnik w celu identyfikacji obiektu. Umożliwia odczyt, a czasami także zapis układu RFID. W zależności od konstrukcji pozwala na odczyt etykiet z odległości do kilkudziesięciu centymetrów lub kilku metrów od anteny czytnika; pl.wikipedia.org/wiki/RFID.

[4] S. Edwards, M. Fortune, *A Guide to RFID in Libraries*, Book Industry Communication, London 2008; V.D. Hunt, A. Puglia, M. Puglia, *RFID – A guide to radio frequency identification*, John Wiley & Sons, Hoboken 2007.

2. Aktualny stan prawny dotyczący dokumentów niejawnych

Przetwarzanie w organizacji dokumentów o różnym poziomie niejawności bazuje na aktualnie obowiązującym stanie prawnym, który określa podstawowe czynności, zasoby i uczestników tych działań. Kluczowym elementem procesu przetwarzania dokumentów jest kancelaria. Wewnątrz każdej kancelarii dochodzi do wielu działań związanych z przetwarzaniem różnego rodzaju dokumentów. Jeśli chodzi o kancelarię tajną (KT), mamy tutaj do czynienia z przetwarzaniem dokumentów o różnym poziomie niejawności. Pośród najważniejszych publikacji znajdują się ustawy i rozporządzenia stanowiące podstawowe źródło badawcze i analityczne. Przy opracowaniu i modelowaniu kancelarii przetwarzającej dokumenty niejawne oraz procesów opisujących zasady i sposoby funkcjonownaia takiej kancelarii wykorzystano aktualnie obowiązujący stan prawny w Polsce[5].

Pojęciu dokumentu wrażliwego nie nadano charakteru definicji legalnej na gruncie przepisów powszechnie obowiązującego prawa. W języku potocznym funkcjonuje jedynie sformułowanie „dane wrażliwe" (inaczej „dane sensytywne") przede wszystkim na określenie danych osobowych. Mowa tutaj będzie zatem o dokumentach zawierających informacje poufne, przeznaczone nie dla nieograniczonego, ale dla wąskiego kręgu odbiorców, z racji na ich charakter oraz potencjalne szkody mogące powstać w przypadku ich ujawnienia. W szerokim tego słowa znaczeniu za dokument wrażliwy można uznać m.in. dokument zawierający dane osobowe, o których mowa w przepisach ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101,

[5] Ustawa o ochronie informacji niejawnych z dnia 5 sierpnia 2010 r. (Dz. U. z 2010 r. Nr 182, poz. 1228), http://isip.sejm.gov.pl/DetailsServlet?id=WDU20101821228 (data odczytu: 01.12.2015); zarządzenie Ministra Obrony Narodowej z dnia 24 grudnia 2013 r. w sprawie szczególnego sposobu organizacji i funkcjonowania kancelarii kryptograficznych (Dz. U. z 2013 r. Nr 46, poz. 401), http://www.dz.urz.mon.gov.pl/dziennik/pozycja/zarzadzenie-401-z-arzadzenie-nr-46mon-z-dnia-24-grudnia-2013-r-w-sprawie-szczegolnego-sposobu-organizacji-i-funkcjonowania-kancelarii-kryptograficznych (data odczytu: 01.12.2015); rozporządzenie Prezesa Rady Ministrów z dnia 7 grudnia 2011 r. w sprawie nadawania, przyjmowania, przewożenia, wydawania i ochrony materiałów zawierających informacje niejawne (Dz. U. z 2011 r. Nr 271, poz. 1603), http://isap.sejm.gov.pl/DetailsServlet?id=WDU20112711603 (data odczytu: 01.12.2015); rozporządzenie Prezesa Rady Ministrów z dnia 7 grudnia 2011 r. w sprawie organizacji i funkcjonowania kancelarii tajnych oraz sposobu i trybu przetwarzania informacji niejawnych (Dz. U. z 2011 r. Nr 276, poz. 1631), http://isap.sejm.gov.pl/DetailsServlet?id=WDU20112761631 (data odczytu: 01.12.2015); rozporządzenie Prezesa Rady Ministrów z dnia 22 grudnia 2011 r. w sprawie sposobu oznaczania materiałów i umieszczania na nich klauzul tajności (Dz. U. z 2011 r. Nr 288, poz. 1692), http://isap.sejm.gov.pl/DetailsServlet?id=WDU20112881692 (data odczytu: 01.12.2015).

poz. 926 z późn. zm.)[6], tajemnicę przedsiębiorstwa, o której mowa w przepisie art. 11 ust. 4 ustawy z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji (Dz. U. z 2003 r. Nr 153, poz. 1503 z późn. zm.)[7], a która obejmuje „nieujawnione do wiadomości publicznej informacje techniczne, technologiczne, organizacyjne przedsiębiorstwa lub inne informacje posiadające wartość gospodarczą, co do których przedsiębiorca podjął niezbędne działania w celu zachowania ich poufności", ale przede wszystkim zawiera „informacje niejawne". Pod pojęciem tych ostatnich będą się zaś kryć, w myśl postanowień przepisu art. 1 ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. z 2010 r. Nr 182, poz. 1228), „informacje, których nieuprawnione ujawnienie spowodowałoby lub mogłoby spowodować szkody dla Rzeczypospolitej Polskiej albo byłoby z punktu widzenia jej interesów niekorzystne, także w trakcie ich opracowywania oraz niezależnie od formy i sposobu ich wyrażania". Te ostanie informacje będą stanowić skądinąd – w świetle dalszych rozważań – zasadniczy element świadczący o „wrażliwym" charakterze dokumentu.

Inaczej rzecz ma się z pojęciem dokumentu, którego definicji legalnej można doszukać się w wielu aktach normatywnych. W art. 115 par. 14 ustawy z dnia 6 czerwca 1997 r. – Kodeks karny (Dz. U. Nr 88, poz. 553 z późn. zm.)[8] stwierdzono: „Dokumentem jest każdy przedmiot lub inny zapisany nośnik informacji, z którym jest związane określone prawo albo który ze względu na zawartą w nim treść stanowi dowód prawa, stosunku prawnego lub okoliczności mającej znaczenie prawne". W art. 3 ust. 1 i 2 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2013 r. poz. 235 z późn. zm.)[9] ustawodawca posługuje się natomiast terminem „dokument elektroniczny", za który uznaje „stanowiący odrębną całość znaczeniową zbiór danych uporządkowanych w określonej strukturze wewnętrznej i zapisany na informatycznym nośniku danych", tj. na „materiale lub urządzeniu służącym do zapisywania, przechowywania i odczytywania danych w postaci cyfrowej".

Zgodnie z postanowieniami przepisu art. 2 pkt 4 ustawy o ochronie informacji niejawnych, stanowiącej podstawę prawną niniejszych rozważań, jest nim natomiast „każda utrwalona informacja niejawna", przy czym na gruncie par. 2 pkt 3 i 4 rozporządzenia Prezesa Rady Ministrów z dnia 22 grudnia 2011 r. w sprawie sposobu oznaczania materiałów i umieszczania na nich klauzul

[6] http://isap.sejm.gov.pl/DetailsServlet?id=WDU20021010926 (data odczytu: 01.12.2015).
[7] http://isap.sejm.gov.pl/DetailsServlet?id=WDU20031531503 (data odczytu: 01.12.2015).
[8] http://isap.sejm.gov.pl/DetailsServlet?id=WDU19970880553 (data odczytu: 01.12.2015).
[9] http://isap.sejm.gov.pl/DetailsServlet?id=WDU20130000235 (data odczytu: 01.12.2015).

tajności (Dz. U. z 2011 r. Nr 288, poz. 1692)[10] dokonano wyodrębnienia pojęć dokumentu elektronicznego i dokumentu nieelektronicznego. Za ten pierwszy uznaje się „dokument utrwalony na informatycznym nośniku danych lub przetwarzany w systemie teleinformatycznym, o ile ze względu na organizację obiegu informacji niejawnych podlega rejestracji", za ten drugi zaś – „dokument utrwalony na nośniku innym niż informatyczny nośnik danych, o ile ze względu na organizację obiegu informacji niejawnych podlega rejestracji".

Stąd też na potrzeby przedmiotowej publikacji, mając na względzie kwestię przetwarzania przez służby mundurowe i specjalne, przyjęto, że pod pojęciem dokumentu wrażliwego kryje się dokument w postaci zarówno przedmiotu, jak i elektronicznego nośnika informacji, którego treść obejmuje przede wszystkim informacje niejawne w świetle ustawy o ochronie informacji niejawnych oraz inne informacje podlegające ochronie z uwagi na zadania realizowane przez służby.

3. Wymagania umożliwiające przetwarzanie dokumentów wrażliwych

Organizacja, w której przewiduje się przetwarzanie dokumentów wrażliwych, musi spełnić odpowiednie wymagania w tym zakresie, wynikające z unormowań prawnych regulujących tę problematykę. Do wymagań tych należy zaliczyć:

- powołanie pełnomocnika do ochrony informacji niejawnych;
- powołanie pionu ochrony w organizacji do realizacji przewidywanych zadań związanych z przetwarzaniem dokumentów wrażliwych w organizacji;
- dostosowanie obiektów organizacji do wymagań w zakresie wytwarzania, przetwarzania, przyjmowania, nadawania, wydawania i ochrony dokumentów wrażliwych wynikające z przepisów prawa;
- zorganizowanie kancelarii tajnej;
- zorganizowanie punktu (miejsca, obiektu) przetwarzania dokumentów wrażliwych, w tym systemów teleinformatycznych służących wykonywaniu i przetwarzaniu dokumentów wrażliwych.

W organizacji, w której przewiduje się przetwarzanie dokumentów wrażliwych, oprócz zatrudnionego pełnomocnika ochrony informacji niejawnych tworzy się pion ochrony, bezpośrednio podległy pełnomocnikowi ochrony informacji niejawnych. W zależności od potrzeb w pionie tym mogą być zatrudnieni:

[10] http://isap.sejm.gov.pl/DetailsServlet?id=WDU20112881692 (data odczytu: 01.12.2015).

- kierownik kancelarii tajnej;
- zastępca kierownika kancelarii tajnej;
- kancelista;
- personel bezpieczeństwa wykonujący czynności związane z fizyczną ochroną informacji niejawnych, w tym kontrolę dostępu do pomieszczeń, w których są przetwarzane informacje niejawne wyłącznie przez osoby uprawnione;
- inspektor bezpieczeństwa teleinformatycznego;
- administrator systemu teleinformatycznego.

Szczegółowe zadania, zakres, normy i procedury dotyczące wymienionych wyżej stanowisk, funkcji, ról i działów organizacji w zakresie zapewnienia niezbędnego poziomu bezpieczeństwa przetwarzania dokumentów wrażliwych oznaczonych klauzulą niejawności zostały przedstawione w raporcie z realizacji zadań projektu „Elektroniczny system zarządzania cyklem życia dokumentów o różnych poziomach wrażliwości", zwanego dalej „projektem RFID"[11].

Obecnie jest możliwe wykorzystanie systemów teleinformatycznych wspomagających funkcjonowanie działów organizacji przetwarzających dokumenty wrażliwe. Stosowanie tego typu systemów wymaga opracowania podstawowych dokumentów bezpieczeństwa teleinformatycznego systemu, do których należą szczególne wymagania bezpieczeństwa systemu teleinformatycznego oraz procedury bezpiecznej eksploatacji. Omówienia natomiast wymaga ich zawartość. Powinny one bowiem zawierać następujące dane:

- w szczególnych wymaganiach bezpieczeństwa:
  1. Charakterystyka systemu: nazwa systemu teleinformatycznego, rodzaje oraz klauzule tajności dokumentów wrażliwych, które będą przetwarzane w systemie teleinformatycznym, przeznaczenie systemu, charakterystyka danych wejściowych i wyjściowych, grupy (kategorie) użytkowników (np. administrator systemu, administrator usługi, aplikacji, urządzenia, inspektor bezpieczeństwa teleinformatycznego, użytkownicy), tryb bezpieczeństwa pracy systemu teleinformatycznego, dokumenty odniesienia.
  2. Budowa systemu: rozmiar systemu, lokalizacja systemu, zasada działania systemu (konfiguracja sprzętowa, konfiguracja programowa, usługi, np. serwis WWW, itp.).

[11] Projekt „Elektroniczny system zarządzania cyklem życia dokumentów o różnych poziomach wrażliwości", realizowany w ramach umowy z Narodowym Centrum Badań i Rozwoju, nr DOBR-BIO4/006/13143/2013 w ramach konkursu związanego z realizacją projektów na rzecz bezpieczeństwa i obronności państwa.

3. Bezpieczeństwo systemu: zarządzanie ryzykiem, krytyczność informacji oraz usług i zasobów, środowiska bezpieczeństwa: środowisko bezpieczeństwa globalnego, środowisko bezpieczeństwa lokalnego, środowisko bezpieczeństwa elektronicznego.
4. Zagrożenia, podatność na ryzyko mające odniesienie do systemu: opis zagrożenia, skutki operacyjne, poziom zagrożenia, poziom podatności, poziom ryzyka, właściciele ryzyka.
5. Środki bezpieczeństwa: organizacyjne środki bezpieczeństwa, środki w zakresie bezpieczeństwa osobowego, środki bezpieczeństwa w zakresie ochrony fizycznej i technicznej odnośnie do: środowiska bezpieczeństwa globalnego, środowiska bezpieczeństwa lokalnego, bezpieczeństwo dokumentów i nośników, w zakresie bezpieczeństwa elektronicznego, ochrony elektromagnetycznej, ochrony kryptograficznej.
6. Ryzyko szczątkowe.
7. Zadania personelu bezpieczeństwa: pełnomocnika ochrony, inspektora bezpieczeństwa teleinformatycznego, administratora systemu, pozostałych osób, którym powierzono zadania w zakresie bezpieczeństwa systemu.
8. Szkolenia.

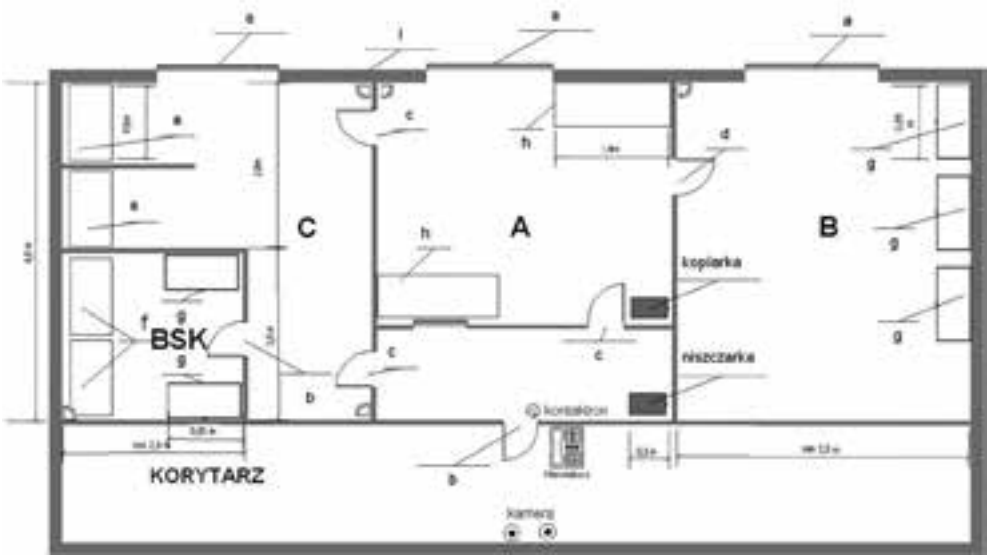
- w procedurach bezpiecznej eksploatacji:
  1. Procedury związane z organizacyjnymi środkami bezpieczeństwa, procedura akredytacji/reakredytacji.
  2. Procedury związane ze środkami bezpieczeństwa fizycznego i technicznego: procedura dostępu do środowiska bezpieczeństwa lokalnego, procedura deponowania nośników danych systemu, procedura nadzoru nad środkami ochrony fizycznej i technicznej, procedura pobierania zapasowych kluczy i kodów, procedura składowania dzienników zdarzeń, procedura postępowania z nośnikami danych.
  3. Procedury związane ze środkami bezpieczeństwa elektronicznego: procedura zakładania i dezaktywacji kont użytkowników, procedura uruchamiania, zamykania systemu i kończenia pracy z systemem, procedura korzystania ze specjalistycznego oprogramowania i usług, procedura importowania danych z innych systemów, procedura eksportowania danych do innych systemów, procedura wykonania kopii zapasowych, procedura informowania o naruszeniu środków bezpieczeństwa elektronicznego, procedura testowania oprogramowania przeznaczonego do użycia w systemie, procedura uaktualniania oprogramowania, procedura wykonania kopii zapasowych systemu, procedura nadzoru nad środkami bezpieczeństwa elektronicznego, procedura pobierania zdeponowanego

hasła administratora, procedura zapewnienia ciągłości działania systemu, procedura wykonania kopii dziennika zdarzeń, procedura bezpieczeństwa przechowywania oprogramowania, procedura przeciwdziałania infekcjom wirusowym, procedura prowadzenia napraw, procedura deklasyfikacji (niszczenia), procedura wycofania z użycia elementów systemu, procedura zakończenia eksploatacji systemu i jego wycofania.

4. Procedury związane z bezpieczeństwem dokumentów: procedura oznaczania, rejestrowania, obiegu oraz niszczenia dokumentów wrażliwych, procedura kontroli dokumentów wytworzonych w systemie, procedura wykonania kopii dokumentów na nośnikach danych, procedura deponowania dysków danych.
5. Procedury związane ze środkami bezpieczeństwa w zakresie ochrony elektromagnetycznej: procedura informowania o nieprawidłowym działaniu lub naruszeniu środków ochrony elektromagnetycznej, procedura nadzoru nad środkami ochrony elektromagnetycznej, procedura naprawy lub wymiany urządzeń klasy TEMPEST, procedury związane z zastosowaniem dodatkowych środków ochrony elektromagnetycznej.
6. Procedury związane ze środkami bezpieczeństwa w zakresie ochrony kryptograficznej: procedura informowania o nieprawidłowym działaniu lub naruszeniu środków ochrony kryptograficznej, procedura nadzoru nad środkami ochrony kryptograficznej, procedura obsługi materiałów kryptograficznych.
7. Procedury alarmowe: procedura na wypadek włamania, procedura na wypadek pożaru, procedura na wypadek zaistnienia zagrożeń środowiskowych, procedura reagowania na incydent komputerowy, procedura odtwarzania działania systemu.
8. Procedura związana z zarządzaniem konfiguracją.
9. Procedura prowadzenia audytów bezpieczeństwa: procedura wykonywania analizy dziennika zdarzeń, procedura dokumentowania analizy dziennika zdarzeń.
10. Obowiązki użytkowników systemu.

4. Przykładowy schemat rozkładu pomieszczeń kancelarii umożliwiającej przyjmowanie, wydawanie, przetwarzanie dokumentów wrażliwych wraz z bezpiecznym stanowiskiem do przetwarzania dokumentów

Rysunek 1 przedstawia przykładowy schemat rozkładu pomieszczeń kancelarii.



A – pomieszczenie pracy personelu, **B** – pomieszczenie magazynowe służące do przechowywania dokumentów wrażliwych, **C** – pomieszczenie umożliwiające zapoznanie się wykonawców (adresatów) z dokumentami wrażliwymi (czytelnia). W ramach pomieszczenia wydzielono pomieszczenie do przetwarzania dokumentów wrażliwych w formie elektronicznej (BSK): a – okna spełniające wymagania (raporty z zadań projektu RFID); b – drzwi spełniające wymagania (raporty z zadań projektu RFID); c, d – drzwi; e – stanowiska do przetwarzania dokumentów wrażliwych o klauzuli „ściśle tajne"; f – bezpieczne stanowisko komputerowe spełniające wymagania dotyczące przetwarzania dokumentów wrażliwych o klauzuli „ściśle tajne"; g – szafy stalowe klasy C – do przechowywania dokumentów wrażliwych oznaczonych klauzulą „ściśle tajne", szafa stalowa klasy B – do przechowywania dokumentów wrażliwych oznaczonych klauzulą „tajne", szafa stalowa klasy A – do przechowywania dokumentów wrażliwych oznaczonych klauzulą „poufne", a także „zastrzeżone"; h – biurka (stanowiska pracy) personelu kancelarii tajnej; i – ściany spełniające wymagania (raporty z zadań projektu RFID).

Rysunek 1. Schemat przykładowego rozkładu pomieszczeń i istotnych urządzeń kancelarii przetwarzającej dokumenty niejawne

Źródło: raporty z zadań projektu RFID.

Pomieszczenie to jest ponadto wyposażone w:

- niszczarkę spełniającą wymagania urządzenia klasy V i VI według normy DIN 32757 – do niszczenia dokumentów wrażliwych o klauzuli „ściśle tajne", a także „tajne", „poufne" i „zastrzeżone";
- kopiarkę spełniającą wymagania do przetwarzania dokumentów wrażliwych w systemach teleinformatycznych;
- system zabezpieczenia przed włamaniem i napadem spełniający wymagania klasy SA4 – powinien sygnalizować nieuprawnione otwarcie drzwi wejściowych i okien oraz próby napadu, instalowane systemy alarmowe powinny spełniać wymagania techniczne i organizacyjne określone w normie obronnej – NO-04-A004. Obiekty wojskowe. Systemy alarmowe;
- telewizyjny system nadzoru, z tym że powinien on rejestrować obraz drzwi wejściowych i osób wchodzących do tych pomieszczeń; instalowane telewizyjne systemy nadzoru powinny spełniać wymagania określone w normie obronnej – NO-04-A004. Obiekty wojskowe. Systemy alarmowe.

Pomieszczenia kancelarii, o ile będzie to możliwe, powinny znajdować się na wyższych kondygnacjach budynku (poza ostatnią kondygnacją) lub w pomieszczeniach piwnicznych (bez okien). Budynek powinien znajdować się na terenie zamkniętym chronionym.

5. Technologia RFID – znakowanie i identyfikacja bezprzewodowa

Technologia znaczników (tagów) RFID umożliwia dość prostą i szybką możliwość znakowania dokumentów, urządzeń i innych obiektów specjalnymi aktywnymi znacznikami. System bezprzewodowego znakowania i identyfikacji jest jednym z elementów składowych systemu mającego zastosowanie w internecie rzeczy (IoT – *Internet of Things*). Technologię RFID w podstawowym układzie tworzą: urządzenie nadawczo-odbiorcze sprzężone z systemem sterującym (tzw. interrogator) oraz etykietą (RFID, NFC label). Budowa etykiety zależy od klasy urządzenia (czyli stopnia zaawansowania układu etykiety). Urządzenia można podzielić na kilka klas, które różnią się zakresem częstotliwości, typem i wielkością pamięci oraz sposobem zasilania. Szczególnie interesujący jest podział tzw. etykiet, które stanowią elementy przenośne bezpośrednio umieszczane na elementach oznakowanych. Podstawowy podział wraz z cechami charakterystycznymi przedstawia tabela 1.

Tabela 1. Klasyfikacja urządzeń technologii RFID

Klasa	Podstawowe własności elementów RFID
I	• etykiety EAS, przeważnie jednobitowe typu *read-only*, • pasywne – brak zasilania autonomicznego, zasilanie z wykorzystaniem energii pola magnetycznego, • zastosowanie główne to znakowanie towarów i zwierząt, • pasmo radiowe: 860–930 MHz
II	• etykiety z dodatkową funkcjonalnością (pamięć, układy kryptograficzne), • w większości przypadków pasywne
III	• etykiety z autonomicznym źródłem zasilania w celu zwiększenia zasięgu
IV	• autonomiczne karty z mikroprocesorem i systemem operacyjnym

Źródło: raporty z zadań projektu RFID.

Do celów transmisji radiowej krótkiego zasięgu stosuje się zwykle częstotliwości nośne: LF (*low frequency*) pasmo 125–134 kHz, HF (*high frequency*) 13.56 MHz, UHF (*ultra high frequency*) 860–960 MHz, Microwave (mikrofalowe) 2.45 GHz lub 5.8 GHz. Najczęściej wykorzystywaną częstotliwością nośną na potrzeby znakowania dokumentów papierowych jest częstotliwość 13.56 MHz. Etykiety zawierają niewiele danych, głównie numer identyfikacyjny, a w zależności od rodzaju pamięci i oczekiwanego zasięgu odpowiedzi można podzielić na:

- pasywne (*passive label*), zasilanie ze źródła sygnału, transmisja danych typu *backscatter* (odbiciowa);
- aktywne (*active label*), zasilanie bateryjne, transmisja danych zasilana z baterii;
- częściowo aktywne (*semi-active label*), zasilanie bateryjne, transmisja danych typu *backscatter*.

Techniki znakowania przy pomocy aktywnych etykiet RFID są obecnie powszechnie stosowane w przemyśle cywilnym i wojskowym. Miniaturyzacja mikrokontrolerów umożliwia znakowanie bardzo małych obiektów na różnych podłożach, w tym także cieczy, np. gazów i lekarstw. Pamięć zastosowana w etykietach może przechowywać dodatkowe informacje, których nie można umieścić np. w kodach kreskowych, tzw. barkodach. Możliwość powiązania techniki RFID z pozycjonowaniem GPS daje nowe możliwości monitorowania obiektów o globalnym zasięgu.

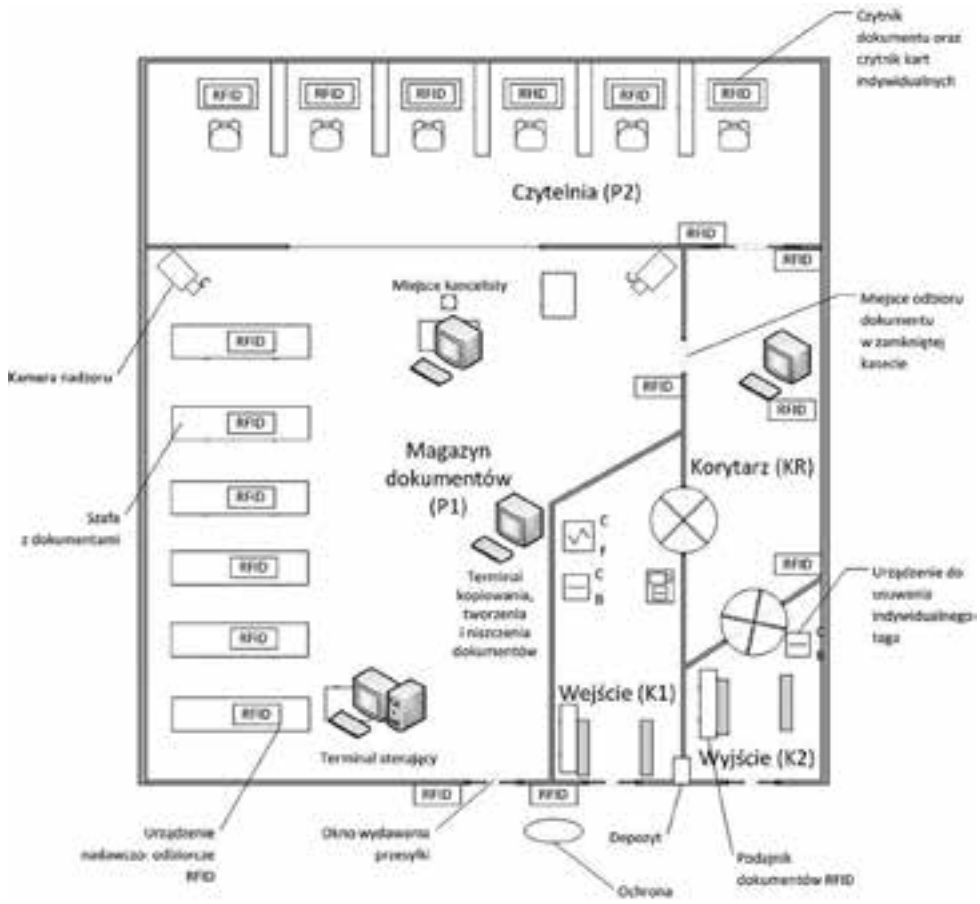
6. Schemat kancelarii przetwarzającej dokumenty wrażliwe oznaczone technologią RFID

Zastosowanie technologii RFID w działaniach kancelarii dokumentów wymaga dokonania jej modernizacji w stosunku do tradycyjnej kancelarii tego typu. Dokumenty i urządzenia oznaczone znacznikami RFID wymagają do obsługi odpowiednich urządzeń i systemów zarządzających. Przykładowy schemat kancelarii przetwarzającej dokumenty wrażliwe jest przedstawiony na rysunku 2. Kancelaria taka powinna spełniać następujące wymagania w zakresie:

- budowy:
  - kancelaria będzie składać się z dwóch pomieszczeń: pomieszczenia, w którym mieszczą się szafy wraz z systemem nadzoru RFID (P1), oraz pomieszczenia zwanego czytelnią dokumentów (P2),
  - kancelaria może posiadać strefę wejściowo-wyjściową lub odrębną: wejście (K1) i wyjście (K2);
- ochrony:
  - przed wejściem znajduje się obligatoryjnie bramka lotniskowa oraz opcjonalnie zestaw biometryczny złożony z co najmniej jednego elementu takiego jak czytnik linii papilarnych, czytnik biometryczny tęczówki oka, czytnik rozkładu naczyń krwionośnych,
  - przed wyjściem znajduje się czytnik RFID,
  - w wyjściu K2 znajduje się bramka lotniskowa (wykrywacz metali),
  - w sali kancelarii (P1) znajduje się monitoring kamer z czujnikami ruchu,
  - każda z szaf w pomieszczeniu (P1) posiada urządzenie nadawczo-odbiorcze przystosowane do pracy na częstotliwościach tagów RFID zastosowanych w dokumentach.

W ramach przykładowego schematu kancelarii zostały użyte urządzenia i systemy pozwalające na efektywne wykorzystanie technologii RFID i typowe funkcjonowanie tego typu działu organizacji. Do tych zasobów zawartych w przykładowym schemacie (rysunek 2) należy zaliczyć:

- 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;



Rysunek 2. Schemat przykładowego rozkładu pomieszczeń i istotnych urządzeń kancelarii przetwarzającej dokumenty wrażliwe oznaczone znacznikami RFID

Źródło: raporty z zadań projektu RFID.

- bramkę wykrywającą 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;
- drukarkę sieciową u kancelisty;
- kserokopiarkę 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 (niszczarka do dokumentów papierowych, niszczarka do płyt CD/DVD, demagnetyzer do dysków HDD itp.).

Należy zaznaczyć, że projekt przewiduje wykorzystanie szaf metalowych, które z jednej strony dają możliwość przechowywania dokumentów o różnych klauzulach niejawności, z drugie zaś – umożliwiają wykorzystanie znaczników RFID w ramach całego proponowanego rozwiązania. W przeszłości jednym z większych problemów w tym obszarze było ich wykorzystania właśnie w metalowych konstrukcjach, które uniemożliwiały odczyt tagów RFID.

7. Podsumowanie i kierunki dalszych badań

Zaproponowany i scharakteryzowany model kancelarii przetwarzającej dokumenty o różnym poziomie wrażliwości z zastosowaniem technologii RFID jest tylko jedną z możliwości wykorzystania tej technologii do przetwarzania dokumentów wrażliwych. Pojęcie kancelarii tajnej jest zwyczajowo związane z podmiotami, które przetwarzają dokumenty zgodnie z ustawą o ochronie informacji niejawnych, natomiast przedstawione rozwiązanie może być również wykorzystane przez podmioty przetwarzające dokumenty zawierające dane istotne z punktu widzenia ich działalności i takie, których ujawnienie mogłoby przynieść określone szkody (głównie dotyczy to szkód finansowych, ale również ujawnienia wrażliwych informacji osobowych). Jednocześnie technologia RFID może zostać wykorzystana do przetwarzania dokumentów, których zagubienie lub zniszczenie mogą powodować określone komplikacje. Przykładem tego rodzaju dokumentów mogą być dowody rzeczowe w sprawach prowadzonych przez sądy lub prokuratury. Innym rodzajem zastosowania może być konieczność znakowania dokumentów związana z ich oryginalnością, czyli przeciwdziałanie wytwarzaniu nielegalnych lub zmodyfikowanych kopii tych dokumentów.

Bibliografia

Edwards S., Fortune M., *A Guide to RFID in Libraries*, Book Industry Communication, London 2008.

Hunt V.D., Puglia A., Puglia M., *RFID – A guide to radio frequency identification*, John Wiley & Sons, Hoboken 2007.

Kiedrowicz M., *Organizacja i dostęp do heterogenicznych, publicznych zasobów danych*, w: *Projektowanie systemów informatycznych: modele i metody*, WAT, Warszawa 2014.

Kiedrowicz M., *Rejestry i zasoby informacyjne wykorzystywane przez organy odpowiedzialne za wykrywanie i przeciwdziałanie przestępczości*, w: *Jawność i jej ograniczenia*, red. G. Szpor, „Monografie Prawnicze", t. 9, *Zadania i kompetencje*, Wydawnictwo C.H. Beck, Warszawa 2015.

Zarządzanie informacjami wrażliwymi – wybrane aspekty organizacyjne, prawne i techniczne ochrony informacji niejawnych, red. M. Kiedrowicz, WAT, Warszawa 2015.

Źródła sieciowe

Rozporządzenie Prezesa Rady Ministrów z dnia 7 grudnia 2011 r. w sprawie nadawania, przyjmowania, przewożenia, wydawania i ochrony materiałów zawierających informacje niejawne (Dz. U. z 2011 r. Nr 271, poz. 1603), http://isap.sejm.gov.pl/DetailsServlet?id=WDU20112711603 (data odczytu: 01.12.2015).

Rozporządzenie Prezesa Rady Ministrów z dnia 7 grudnia 2011 r. w sprawie organizacji i funkcjonowania kancelarii tajnych oraz sposobu i trybu przetwarzania informacji niejawnych (Dz. U. z 2011 r. Nr 276, poz. 1631), http://isap.sejm.gov.pl/DetailsServlet?id=WDU20112761631 (data odczytu: 01.12.2015).

Rozporządzenie Prezesa Rady Ministrów z dnia 22 grudnia 2011 r. w sprawie sposobu oznaczania materiałów i umieszczania na nich klauzul tajności (Dz. U. z 2011 r. Nr 288, poz. 1692), http://isap.sejm.gov.pl/DetailsServlet?id=WDU20112881692 (data odczytu: 01.12.2015).

Ustawa z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji (Dz. U. z 2003 r. Nr 153, poz. 1503 z późn. zm.), http://isap.sejm.gov.pl/DetailsServlet?id=WDU20031531503 (data odczytu: 01.12.2015).

Ustawa z dnia 6 czerwca 1997 r. – Kodeks karny (Dz. U. z 1997 r. Nr 88, poz. 553 z późn. zm.), http://isap.sejm.gov.pl/DetailsServlet?id=WDU19970880553 (data odczytu: 01.12.2015).

Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926 z późn. zm.), http://isap.sejm.gov.pl/DetailsServlet?id=WDU20021010926 (data odczytu: 01.12.2015).

Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2013 r. poz. 235 z późn. zm.), http://isap.sejm.gov.pl/DetailsServlet?id=WDU20130000235 (data odczytu: 01.12.2015).

Ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. z 2010 r. Nr 182, poz. 1228), http://isip.sejm.gov.pl/DetailsServlet?id=WDU20101821228 (data odczytu: 01.12.2015).

Zarządzenie Ministra Obrony Narodowej z dnia 24 grudnia 2013 r. w sprawie szczególnego sposobu organizacji i funkcjonowania kancelarii kryptograficznych (Dz. U. z 2013 r. Nr 46, poz. 401), http://www.dz.urz.mon.gov.pl/dziennik/pozycja/zarzadzenie-401-zarzadzenie-nr-46mon-z-dnia-24-grudnia-2013-r-w-sprawie-szczegolnego-sposobu-organizacji-i-funkcjonowania-kancelarii-kryptograficznych (data odczytu: 01.12.2015).

* * *

Secret office model for the processing of classified documents using RFID technology

Summary

This article presents a new model for the secret office that processes documents with varying levels of sensitivity, supported by an IT workflow system and RFID technology. The secret office model was developed using the current status of the law in Poland.

Keywords: workflow system, document processing, RFID