KAP-4101-002-00/2014
Nr ewid. 205/2014/P/14/004/KAP

Informacja o wynikach kontroli

WDRAŻANIE WYBRANYCH WYMAGAŃ DOTYCZĄCYCH SYSTEMÓW TELEINFORMATYCZNYCH, WYMIANY INFORMACJI W POSTACI ELEKTRONICZNEJ ORAZ KRAJOWYCH RAM INTEROPERACYJNOŚCI NA PRZYKŁADZIE NIEKTÓRYCH URZĘDÓW GMIN MIEJSKICH I MIAST NA PRAWACH POWIATU

DEPARTAMENT
ADMINISTRACJI PUBLICZNEJ

MISJĄ

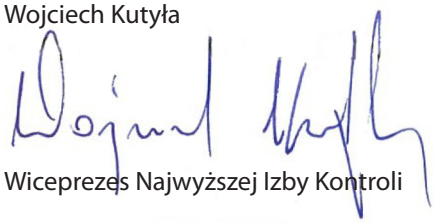
Najwyższej Izby Kontroli jest dbałość o gospodarność i skuteczność w służbie publicznej dla Rzeczypospolitej Polskiej

WIZJĄ

Najwyższej Izby Kontroli jest cieszący się powszechnym autorytetem najwyższy organ kontroli państwowej, którego raporty będą oczekiwanym i poszukiwanym źródłem informacji dla organów władzy i społeczeństwa

Dyrektor
Departamentu Administracji Publicznej:
Bogdan Skwarka

Akceptuję:
Wojciech Kutyła



Wiceprezes Najwyższej Izby Kontroli

Zatwierdzam:
Krzysztof Kwiatkowski

Prezes Najwyższej Izby Kontroli
Warszawa, dnia 2 lutego 2015 r.

Najwyższa Izba Kontroli
ul. Filtrowa 57
02-056 Warszawa
T/F +48 22 444 50 00

www.nik.gov.pl

Spis treści

Zdjęcie na okładce:
Anna Demus

Wykaz stosowanych skrótów i pojęć

BIP	Biuletyn Informacji Publicznej
CRD	centralne repozytorium wzorów dokumentów elektronicznych
ePUAP	Elektroniczna Platforma Usług Administracji Publicznej. System teleinformatyczny udostępniający usługi elektroniczne administracji publicznej dla obywateli
KRI – Krajowe Ramy Interoperacyjności	stanowią zbiór zasad i sposobów postępowania podmiotów w celu zapewnienia systemom informatycznym interoperacyjności działania, rozumianej jako zdolność tych systemów oraz wspieranych przez nie procesów do wymiany danych oraz do dzielenia się informacjami i wiedzą
MAiC	Ministerstwo Administracji i Cyfryzacji
RI – repozytorium interoperacyjności	część zasobów ePUAP przeznaczona do udostępniania informacji służących osiąganiu interoperacyjności
rozporządzenie ePUAP	rozporządzenie Ministra Administracji i Cyfryzacji z dnia 6 maja 2014 r. w sprawie zakresu i warunków korzystania z elektronicznej platformy usług administracji publicznej[1], które weszło w życie z dniem 11 maja 2014 r.; poprzednio obowiązywało rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 27 kwietnia 2011 r. w sprawie zakresu i warunków korzystania z elektronicznej platformy usług administracji publicznej[2]
rozporządzenie KRI	rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych[3]
rozporządzenie w sprawie instrukcji kancelaryjnej	rozporządzenie Prezesa Rady Ministrów z dnia 18 stycznia 2011 r. w sprawie instrukcji kancelaryjnej, jednolitych rzeczowych wykazów akt oraz instrukcji w sprawie organizacji i zakresu działania archiwów zakładowych[4]
UM	Urząd Miejski/Urząd Miasta
ustawa o NIK	ustawa z dnia 23 grudnia 1994 r. o Najwyższej Izbie Kontroli[5]
ustawa o informatyzacji	ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne[6]
XML	*(eXtensible Markup Language)* – tekstowy format służący do opisywania informacji (danych) w sposób strukturalny; jest to format, przy pomocy którego nadaje się znaczenie poszczególnym fragmentom informacji
PDF	format plików służący do prezentacji, przenoszenia i drukowania treści tekstowo-graficznych, stworzony i promowany przez firmę Adobe Systems; format PDF powstał jako format wynikowy, mający zachować pełny wygląd dokumentu po wydrukowaniu

1 Dz. U. z 2014 r., poz. 584.
2 Dz. U. Nr 93, poz. 546.
3 Dz. U. z 2012 r., poz. 526 ze zm.
4 Dz. U. z 2011 r., Nr 14, poz. 67 ze zm.
5 Dz. U. z 2012 r., poz. 82 ze zm.
6 Dz. U. z 2014 r., poz. 1114.

dostępność	właściwość bycia dostępnym i możliwym do wykorzystania na żądanie, w założonym czasie, przez autoryzowany podmiot
integralność	zapewnienie dokładności i kompletności informacji oraz metod jej przetwarzania
interoperacyjność	zdolność różnych podmiotów oraz używanych przez nie systemów teleinformatycznych i rejestrów publicznych do współdziałania na rzecz osiągnięcia wzajemnie korzystnych i uzgodnionych celów, z uwzględnieniem współdzielenia informacji i wiedzy przez wspierane przez nie procesy biznesowe realizowane za pomocą wymiany danych za pośrednictwem wykorzystywanych przez te podmioty systemów teleinformatycznych[7]; osiąganie interoperacyjności następuje poprzez ciągłe doskonalenie jednostki w zakresie zarządzania systemami informatycznymi
model usługowy	jest modelem architektury systemu informatycznego, w którym dla użytkowników (klientów/odbiorców) zdefiniowano stanowiące odrębną całość funkcje systemu teleinformatycznego (usługi sieciowe) oraz opisano sposób korzystania z tych funkcji
polityka bezpieczeństwa informacji	zestaw praw, reguł i praktycznych doświadczeń, regulujących sposób zarządzania, ochrony i dystrybucji informacji wewnątrz określonego systemu
poufność	zapewnienie, że informacja jest dostępna tylko dla osób do tego upoważnionych
usługa elektroniczna	w myśl art. 2 pkt 4 ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną[8], jest to usługa świadczona bez jednoczesnej obecności stron (na odległość), poprzez przekaz danych na indywidualne żądanie usługobiorcy, przesyłanej i otrzymywanej za pomocą urządzeń do elektronicznego przetwarzania
współdzielenie informacji	wspólne użytkowanie tych samych zasobów przez różne osoby i/lub podmioty, np. zasobów takich jak: pliki, bazy danych, dokumenty itp.

7 Źródło: art. 3 pkt 18 ustawy o informatyzacji.

8 Dz. U. z 2013 r., poz. 1422.

1 ZAŁOŻENIA KONTROLI

1.1 Temat i numer kontroli

Wdrażanie wybranych wymagań dotyczących systemów teleinformatycznych, wymiany informacji w postaci elektronicznej oraz Krajowych Ram Interoperacyjności na przykładzie niektórych urzędów gmin miejskich i miast na prawach powiatu (P/14/004).

1.2 Wprowadzenie oraz uzasadnienie podjęcia kontroli

Przepisy dotyczące interoperacyjności mają na celu stworzenie warunków do współdziałania ze sobą systemów informatycznych jednostek realizujących zadania publiczne dla zapewnienia szybkiej wymiany informacji zarówno wewnątrz urzędu jak i z innymi urzędami administracji publicznej. Wdrożenie tych przepisów powinno przyczynić się do usprawnienia realizacji zadań urzędów, w tym załatwiania spraw obywateli i przedsiębiorców, które będą mogły być załatwiane sprawniej, tj. na odległość i w krótszym czasie, bez żądania informacji będących już w posiadaniu urzędów.

Osiągnięcie interoperacyjności nie jest jednorazowym, lecz ciągłym procesem zależnym od wielu czynników m.in. od zmian w środowisku informatycznym. Interoperacyjności nie osiąga się jednorazowo na długi czas. Jest to proces wymagający stałego monitorowania, biorąc pod uwagę dostępność zbiorów danych, zmianę zachowań użytkowników i wprowadzanie nowych programów, technologii oraz urządzeń informatycznych.

Ustawa o informatyzacji w art. 13 nałożyła na podmioty realizujące zadania publiczne obowiązki w celu osiągnięcia minimalnego stanu zgodności technicznej systemów teleinformatycznych, który umożliwi współpracę używanych przez nie systemów, co powinno zapewnić sprawny przepływ informacji oraz zwiększyć szybkość i skuteczność działania tych podmiotów. Rozporządzenie KRI wykonuje upoważnienie ustawowe zawarte w art. 18 ustawy o informatyzacji w zakresie minimalnych wymagań dla systemów informatycznych, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz Krajowych Ram Interoperacyjności.

Wraz z rozwojem elektronicznej formy komunikacji znaczenia nabiera zapewnienie dostępności, integralności i poufności danych posiadanych i przetwarzanych przez urzędy. Dlatego też, szczególnie istotnym jest zapewnienie bezpieczeństwa informacji przetwarzanych w użytkowanych przez podmioty publiczne systemach informatycznych. W przeciwnym razie powstaje ryzyko utraty ww. właściwości gwarantujących bezpieczeństwo informacji, a w konsekwencji stabilności pracy urzędów. Podważyć to może zaufanie obywateli do organów administracji publicznej. Jednostka, aby zabezpieczyć swoje informacje powinna zastosować podejście systemowe, w ramach którego będzie zarządzać kompleksowo posiadanymi aktywami informacyjnymi, infrastrukturą przeznaczoną do ich przetwarzania oraz ryzykiem dotyczącym bezpieczeństwa informacji. Podstawowe wymagania w zakresie systemu zarządzania bezpieczeństwem informacji reguluje § 20 rozporządzenia KRI.

W kontekście dostępności informacji dla wszystkich obywateli istotne jest wprowadzanie rozwiązań technicznych umożliwiających korzystanie z nich przez osoby niepełnosprawne. Stąd informacje udostępniane na stronach internetowych urzędów powinny charakteryzować się także pełną czytelnością dla osób niepełnosprawnych.

W strategicznym dokumencie opisującym zamierzenia rządu dla dostarczenia społeczeństwu wysokiej jakości elektronicznych usług publicznych jakim jest *Program Zintegrowanej Informatyzacji Państwa*[9] (dalej PZIP) wskazano m.in., że:

[9] Przyjęty przez Radę Ministrów w dniu 8 stycznia 2014 r., https://mac.gov.pl/files/pzip_ostateczny.pdf.

Celem administracji publicznej powinno być budowanie nowych i modernizacja istniejących systemów teleinformatycznych w taki sposób, aby były one ze sobą spójne i logicznie powiązane oraz zorientowane na potrzeby użytkownika. Spełnienie wymagań w zakresie interoperacyjności będzie jednym z kluczowych kryteriów warunkujących decyzję o budowie systemu teleinformatycznego. Dzięki temu w ramach systemu informacyjnego państwa będzie ułatwione korzystanie ze spójnych danych, zgromadzonych w różnych rejestrach i systemach ewidencyjnych, przy realizacji różnych usług.

Wskazano w nim również, że interoperacyjność systemów i rozwiązań teleinformatycznych stanowi jeden z głównych elementów, który stworzy warunki dla rozwoju rynku usług świadczonych drogą elektroniczną obywatelom i przedsiębiorcom. Zapewnienie interoperacyjności powinno przyczynić się do efektywnego świadczenia usług publicznych, co jest jednym z celów założonych w *Strategii Sprawne Państwo 2020*[10]. Zagadnienia współdziałania różnych systemów informatycznych (interoperacyjności) oraz elektronicznego zarządzania dokumentami zostały również uwzględnione w Programie Operacyjnym *Polska Cyfrowa PO PC 2014–2020*[11] (dalej *PO PC*). W dokumencie tym wskazano, że są one istotne dla usprawnienia pracy administracji publicznej, aby szybciej i taniej załatwiać sprawy obywateli.

Tematyka dotycząca wykonywania zadań w zakresie realizacji wymagań wprowadzonych rozporządzeniem KRI nie była wcześniej przedmiotem badania przez NIK z uwagi na wejście w życie tego rozporządzenia z dniem 31 maja 2012 r. Przeprowadzenie tej kontroli miało na celu zbadanie w urzędach miast i miast na prawach powiatu podejmowanych działań dla spełnienia wymogów nałożonych rozporządzeniem KRI.

Kontrola została podjęta z inicjatywy własnej NIK, a temat kontroli mieści się w ramach priorytetowego kierunku kontroli NIK *Poprawa obsługi obywateli przez administrację publiczną,* przyjętego w planie pracy NIK na 2014 r.

1.3 Cel kontroli

Celem kontroli NIK była ocena wdrażania wybranych wymagań określonych w rozporządzeniu KRI. W związku z tym ocenie poddano następujące, wybrane kwestie:

- prawidłowość realizacji przez Ministra Administracji i Cyfryzacji zadań określonych w rozporządzeniu KRI, w szczególności w zakresie prowadzenia repozytorium interoperacyjności oraz publicznej dyskusji nad rekomendacjami dotyczącymi interoperacyjności;
- działania burmistrzów oraz prezydentów miast w celu realizacji wymagań wprowadzonych rozporządzeniem KRI, dotyczących w szczególności:
  - dostosowania posiadanych systemów informatycznych do współpracy z innymi systemami/rejestrami informatycznymi,
  - stopnia wdrożenia systemu zarządzania bezpieczeństwem systemów informatycznych.

Ponadto, zbadano działania w celu zapewnienia dostępności informacji dla osób niepełnosprawnych.

[10] Uchwała Nr 17 Rady Ministrów z dnia 12 lutego 2013 r. w sprawie przyjęcia strategii „Sprawne Państwo 2020" (M.P. z 2013 r., poz. 136).

[11] http://www.mir.gov.pl/aktualnosci/fundusze_europejskie/Strony/Program_Polska_Cyfrowa_przyjety_przez_KomisjeEuropejska_51214.aspx PO PC po negocjacjach został zatwierdzony w dniu 5 grudnia 2014 r. przez Komisję Europejską.

1.4 Organizacja i zakres kontroli

Kontrolę przeprowadzono w 25 jednostkach, tj. w: MAiC oraz w 24 wybranych urzędach gmin miejskich i miast na prawach powiatu w województwach: dolnośląskim, małopolskim, mazowieckim, śląskim, wielkopolskim i zachodniopomorskim. Wykaz jednostek objętych kontrolą stanowi załącznik nr 2 do Informacji. Wyboru jednostek do kontroli dokonano w sposób celowy. Wybór jednostek wynikał z założenia, że w większych jednostkach samorządowych istnieje większe prawdopodobieństwo modernizacji lub zakupu systemów informatycznych, które będą podlegały wymogom rozporządzenia KRI, obowiązującego od 31 maja 2012 r., co umożliwiało przeprowadzenie pełnego zakresu badań kontrolnych.

Kontrolę w MAiC przeprowadzono na podstawie art. 2 ust. 1 ustawy o NIK, z uwzględnieniem kryteriów określonych w art. 5 ust. 1 ww. ustawy, tj. pod względem legalności, gospodarności, rzetelności i celowości. W jednostkach samorządu terytorialnego kontrolę przeprowadzono na podstawie art. 2 ust. 2 w związku z art. 5 ust. 2 ustawy o NIK, tj. pod względem legalności, rzetelności i gospodarności.

Kontrolą objęto okres od dnia wejścia w życie rozporządzenia KRI, tj. od 31 maja 2012 r. do dnia zakończenia czynności kontrolnych w 2014 r. Czynności kontrolne przeprowadzono w okresie od 8 czerwca do 24 października 2014 r.

2 PODSUMOWANIE WYNIKÓW KONTROLI

2.1 Ocena kontrolowanej działalności[12]

W ocenie Najwyższej Izby Kontroli Minister Administracji i Cyfryzacji wywiązał się z zadań wynikających z rozporządzenia KRI, dotyczących w szczególności prowadzenia publicznej dyskusji nad rekomendacjami interoperacyjności i ich publikowania oraz umożliwienia jednostkom administracji publicznej zamieszczania w centralnym repozytorium wzorów dokumentów elektronicznych na ePUAP wzorów dokumentów elektronicznych wykorzystywanych w procesie świadczenia usług elektronicznych. Podejmowano również działania mające na celu zapoznanie przedstawicieli administracji publicznej z zagadnieniami interoperacyjności systemów informatycznych.

Stwierdzono natomiast, że Minister Administracji i Cyfryzacji nie podejmował kontroli w podmiotach publicznych w zakresie działania systemów teleinformatycznych, prowadzenia rejestrów i wymiany informacji w postaci elektronicznej, przewidzianych w art. 25 ust. 1 pkt 3 lit. c ustawy o informatyzacji.

Najwyższa Izba Kontroli, pozytywnie ocenia działania podjęte przez burmistrzów i prezydentów miast w celu dostosowania objętych kontrolą systemów teleinformatycznych[13] do współpracy z innymi systemami/rejestrami, jednakże NIK sformułowała wiele uwag w tym zakresie. Większość z kontrolowanych systemów informatycznych (72 z 77) współpracowało z innymi systemami informatycznymi urzędów i tym samym spełniało minimalne wymogi interoperacyjności, o których mowa w § 5 ust. 3 pkt 3 rozporządzenia KRI. Niemniej tylko dwanaście (16,7%) systemów współpracowało z innymi systemami urzędu w sposób w pełni zautomatyzowany, tj. na poziomie najbardziej pożądanym, a pięć systemów (6,9%) bezpośrednio korzystało z danych gromadzonych w zewnętrznych systemach/rejestrach publicznych (zasada referencji), takich jak np. rejestr centralny PESEL[14] czy też System Informacji Przestrzennej.

NIK, ze względu na liczne nieprawidłowości, ogólnie negatywnie ocenia działania burmistrzów i prezydentów miast w zakresie zarządzania bezpieczeństwem informacji w urzędach, o którym mowa w § 20 rozporządzenia KRI. NIK stwierdziła nieprawidłowości w tym obszarze w 21[15] z 24 (87,5%) skontrolowanych urzędów miast, z których sześć oceniła negatywnie[16]. Zdaniem NIK, stwierdzone nieprawidłowości mogą skutkować utratą dostępności, integralności i poufności informacji przetwarzanych w systemach informatycznych urzędów wykorzystywanych do elektronicznej komunikacji i świadczenia usług. Nieprawidłowości dotyczyły przede wszystkim:

- braku w kontrolowanych urzędach całościowej Polityki Bezpieczeństwa Informacji (poza bezpieczeństwem danych osobowych), która jest wymagana przepisami § 20 ust. 1 i 3 rozporządzenia KRI;

---

12 NIK zastosowała w kontroli następującą skalę ocen: pozytywna, negatywna, opisowa. Opisową formę oceny ogólnej kontrolowanej działalności stosowano wtedy, gdy działania lub stwierdzone nieprawidłowości w poszczególnych obszarach objętych kontrolą nie dawały podstaw do ogólnej oceny pozytywnej, jak również nie uzasadniały wydania ogólnej oceny negatywnej.

13 Kontrolą objęto wybrane systemy informatyczne zakupione lub istotnie zmodernizowane po wejściu w życie rozporządzenia KRI, tj. po 31 maja 2012 r.

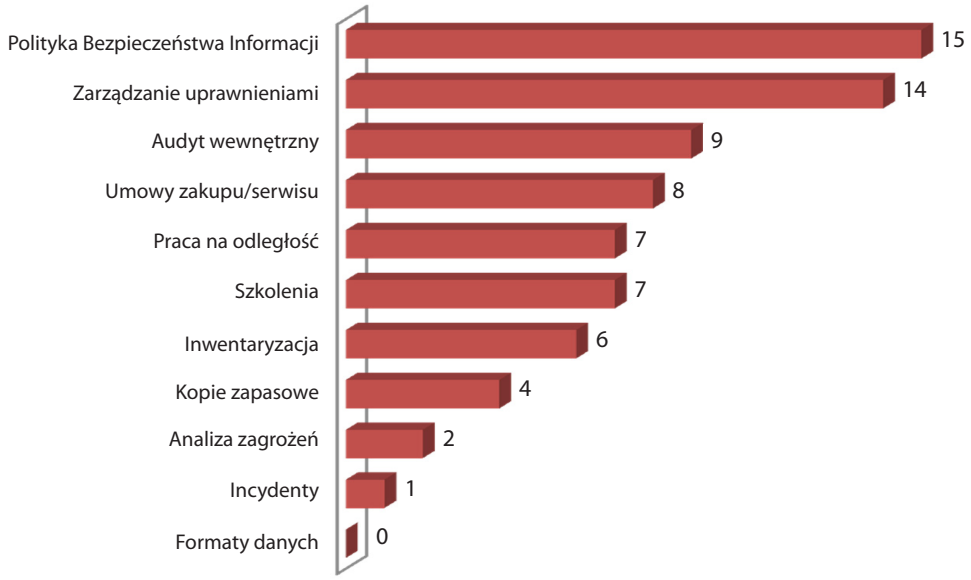
14 PESEL – Powszechny Elektroniczny System Ewidencji Ludności. Zawiera dane osób zameldowanych na pobyt stały lub czasowy trwający ponad 3 miesiące, osób ubiegających się o wydanie dowodu osobistego lub paszportu, a także osób, dla których odrębne przepisy przewidują potrzebę posiadania numeru PESEL (źródło: https://msw.gov.pl/pl/sprawy-obywatelskie/centralne-rejestry-pan/32,PESEL.html).

15 Z wyjątkiem UM w: Legnicy, Mysłowicach i Świdnicy.

16 UM w: Głogowie, Mińsku Mazowieckim, Nowym Targu, Olkuszu, Pruszkowie i Świnoujściu.

- niewłaściwego zarządzania uprawnieniami użytkowników w zakresie dostępu do systemów informatycznych, co było niezgodne z § 20 ust. 2 pkt 4 i 5 rozporządzenia KRI;
- nieprzeprowadzania corocznych audytów wewnętrznych z zakresu bezpieczeństwa informacji, co było niezgodne z § 20 ust. 2 pkt 14 rozporządzenia KRI;
- braku w umowach na zakup lub serwis sprzętu komputerowego/oprogramowania zapisów gwarantujących zabezpieczenie poufności informacji uzyskanych w związku z realizacją tych umów przez wykonawców, co było niezgodne z § 20 ust. 2 pkt 10 rozporządzenia KRI.

Wykres nr 1
Liczba kontrolowanych urzędów, w których stwierdzono nieprawidłowości przy realizacji poszczególnych zadań w obszarze zarządzania bezpieczeństwem informacji



Źródło: Wyniki kontroli.

Biorąc pod uwagę, że wymagania w zakresie dostosowania sposobu prezentacji informacji przez systemy informatyczne do potrzeb osób niepełnosprawnych określone w § 19 rozporządzenia KRI mają być ostatecznie wprowadzone do dnia 31 maja 2015 r., NIK nie dokonywała oceny działalności kontrolowanych jednostek w tym obszarze. Wyniki kontroli wykazały, że we wszystkich kontrolowanych urzędach występowały na ich stronach internetowych i/lub na stronach BIP błędy związane z prezentowaniem treści dla osób niepełnosprawnych.

2.2 Synteza wyników kontroli

2.2.1. Realizacja zadań przez Ministra Administracji i Cyfryzacji w zakresie interoperacyjności systemów informatycznych

W MAiC w okresie objętym kontrolą:

- zapewniono prowadzenie publicznej dyskusji nad rekomendacjami interoperacyjności na Portalu Interoperacyjności, udostępnionym na platformie ePUAP, stosownie do § 9 pkt 1 rozporządzenia KRI [str. 20];

- zapewniono prowadzenie repozytorium interoperacyjności, w którym zamieszczono informację o 26 rekomendacjach interoperacyjności[17], w tym o rekomendacjach dotyczących standardu Elektronicznej Skrzynki Podawczej (dalej ESP) oraz standardu Formularza ePUAP, stosownie do § 9 pkt 2 rozporządzenia KRI [str. 21];
- opublikowano w repozytorium interoperacyjności na ePUAP schematy XML struktury danych cech informacyjnych obiektów[18], zgodnie z § 10 ust. 5 rozporządzenia KRI [str. 21];
- przeprowadzano szkolenia dotyczące interoperacyjności oraz udzielano na bieżąco (z wyjątkiem jednego przypadku) informacji i wyjaśnień w sprawach regulowanych rozporządzeniem KRI [str. 21–22].

Kontrola wykazała jednak, że Minister Administracji i Cyfryzacji:

- nie planował i nie przeprowadzał kontroli interoperacyjności systemów informatycznych w podmiotach publicznych, tj. nie realizował zadania określonego w art. 25 ust. 1 pkt 3 lit. c ustawy o informatyzacji [str. 23–24];
- nie przekazał wojewodom jednolitych kryteriów merytorycznych sposobu realizacji obowiązku określonego w art. 25 ust. 1 pkt 3 lit. a ustawy o informatyzacji, dotyczącego przeprowadzania kontroli w jednostkach samorządu terytorialnego w zakresie działania systemów teleinformatycznych oraz rejestrów publicznych, które są używane do realizacji zadań zleconych z zakresu administracji rządowej [str. 22];
- nie w pełni zrealizował określone w Programie Zintegrowanej Informatyzacji Państwa krótkookresowe zadania w obszarze interoperacyjności, pomimo upływu sześciomiesięcznego terminu na ich realizację określonego w tym Programie [str. 24–26].

Ponadto, kontrola wykazała, że w MAiC nie wypracowano jednoznacznego stanowiska w sprawie znaczenia terminu „istotnej modernizacji" systemu informatycznego, o której mowa w § 23 rozporządzenia KRI, pomimo zgłaszanych wątpliwości przez podmioty publiczne. W opinii NIK, brak precyzyjnego określenia pojęcia „istotnej modernizacji" powoduje, że podmioty realizujące zadania publiczne nie potrafią ocenić czy zakres modernizacji jest na tyle istotny, że stwarza obowiązek dostosowania systemu informatycznego do wymogów zawartych w rozdziale IV rozporządzenia KRI [str. 22–23].

2.2.2. Dostosowanie przez kontrolowane urzędy gmin miejskich i miast na prawach powiatu posiadanych systemów informatycznych do współpracy z innymi systemami/rejestrami informatycznymi

- **W większości z kontrolowanych urzędów (22 spośród 24, tj. 91,7%) w dokumentach strategicznych uwzględniano m.in. rozbudowę infrastruktury teleinformatycznej i wykorzystanie nowoczesnych technologii w komunikacji mieszkańców z urzędem**[19] [str. 26]. W strategiach określano też cele i zadania dotyczące rozwoju usług informatycznych. Pomimo takich założeń, tylko w nielicznych urzędach (cztery) podejmowano aktywne działania dla poznania potrzeb mieszkańców w zakresie korzystania z elektronicznych form komunikacji z urzędem [str. 26–27].

[17] Rekomendacja to dokument wypracowany w ramach Portalu Interoperacyjności. W ramach jednej rekomendacji mogą powstać różne produkty (np. schemat XML).

[18] Jest to standard wymiany plików używany w komunikacji między systemami informatycznymi, przyjęty do stosowania w administracji publicznej.

[19] Zagadnień dotyczących dostosowania urzędu do elektronicznego świadczenia usług publicznych nie zawarto w dokumentacji strategicznej dwóch miast tj. „Strategii Rozwoju Gminy Zawiercie 2025 plus" i w „Strategii Rozwoju Miasta Mińsk Mazowiecki do roku 2020".

- **W mniej niż połowie skontrolowanych urzędów (w 11 z 24, tj. 45,8%) podejmowano działania mające na celu promowanie komunikacji elektronicznej z urzędem, w tym możliwości korzystania z udostępnionych usług elektronicznych.** NIK zwraca uwagę na potrzebę podjęcia przez urzędy szerszych działań w zakresie informowania o e-usługach i ich promowania, co mogłoby wpłynąć na większe zainteresowanie mieszkańców możliwością załatwiania spraw w urzędzie drogą elektroniczną. Ma to szczególne znaczenie w sytuacji gdy liczba złożonych dokumentów w tej formie jest znikoma i gdy urzędy świadczą usługi w formie elektronicznej [str. 26–27].
- **W 22 z 24 (91,7%) kontrolowanych urzędów jako podstawowy sposób dokumentowania przebiegu rozpatrywania i rozstrzygania spraw, wskazywano system tradycyjny (papierowy) wykonywania czynności kancelaryjnych w urzędzie.** W dwóch pozostałych urzędach[20] jako podstawowy sposób dokumentowania przebiegu załatwiania i rozstrzygania spraw, wskazany został system elektronicznego zarządzania dokumentacją. W 18 z 22 urzędów (81,8%) system tradycyjny wykonywania czynności kancelaryjnych wspomagany był przez elektroniczne systemy obiegu dokumentów na różnych etapach załatwiania spraw w urzędzie. Zdaniem NIK, wykorzystywanie systemu tradycyjnego obiegu dokumentów równolegle z elementami obiegu elektronicznego, powoduje że te same czynności są częściowo powielane, co niewątpliwie ma wpływ na większe obciążenie pracą urzędników. Istotą wprowadzenia elektronicznego obiegu dokumentów jest usprawnienie i przyśpieszenie obiegu informacji przy jednoczesnej minimalizacji nakładu pracy. Wskazane jest zatem, aby kontynuować działania w celu zapewnienia technicznych i organizacyjnych warunków dla wprowadzenia w urzędach wyłącznie elektronicznego systemu zarządzania dokumentacją, co spowoduje również zmniejszenie zużycia papieru i korzystnie wpłynie na ochronę środowiska [str. 27–28].
- **W sześciu z 18 urzędów (33,3%), w których pomocniczo wykorzystywano system elektronicznego obiegu dokumentów, nie wprowadzono procedur określających zasady ich obiegu w urzędzie.** Zdaniem NIK, zasadnym jest opracowanie odpowiednich procedur elektronicznego obiegu dokumentów uwzględniających przyjętą praktykę postępowania. Wdrożenie takiej procedury wpłynie zarówno na uporządkowanie i usprawnienie obiegu dokumentów, a także pozwoliłoby na wyeliminowanie równoległego przesyłania dokumentów papierowych i elektronicznych [str. 29].
- **Dominującą formą korespondencji w urzędach była korespondencja tradycyjna (papierowa).** Stanowiła ona aż 94% ogółu korespondencji wpływającej i wychodzącej [str. 29].
- **Wszystkie objęte badaniem urzędy świadczyły usługi w formie elektronicznej.** Liczba świadczonych usług była jednak bardzo zróżnicowana i kształtowała się od jednej usługi, tj. Elektronicznej Skrzynki Podawczej (świadczonej przez cztery urzędy[21]), do ponad 100 usług (świadczonych przez UM w: Dąbrowie Górniczej i Mysłowicach). Łącznie w skontrolowanych urzędach udostępniono 554 e-usługi świadczone na ogólnopolskiej platformie ePUAP, w tym również z wykorzystaniem platform regionalnych, takich jak SEKAP[22] i Cyfrowa Małopolska[23]

20 UM w: Głogowie i Zawierciu.

21 UM w: Lesznie, Mińsku Mazowieckim, Stargardzie Szczecińskim, Szczecinku.

22 System Elektronicznej Komunikacji Administracji Publicznej – projekt samorządów gmin i powiatów województwa śląskiego.

23 Cyfrowa Małopolska to platforma informatyczna stworzona dla województwa małopolskiego.

oraz platform miejscowych, np. Płocka Platforma Teleinformatyczna e-Urząd, a także stron internetowych urzędów. Zaznaczyć należy, że największą liczbę usług elektronicznych świadczyły ww. dwa urzędy z terenu województwa śląskiego z wykorzystaniem platformy SEKAP [str. 30–31].

- **W większości przypadków (98 usług z próby 114 usług elektronicznych objętych badaniem) zamieszczone na stronach internetowych i BIP urzędów opisy e-usług zawierały wymagane informacje określone w rozporządzeniu ePUAP**[24]. W przypadku 16 usług opisy zawierały nieaktualne lub niekompletne podstawy prawne [str. 31–32]. Dwa urzędy[25] na swoich stronach BIP nie zamieściły dla badanych usług elektronicznych informacji odnośnie obowiązujących procedur w zakresie załatwiania spraw drogą elektroniczną, co było niezgodne z § 5 ust. 2 pkt 4 rozporządzenia KRI [str. 32].
- **Siedem urzędów**[26] **nie przekazało wzorów dokumentów elektronicznych do CRD** (spośród 11 urzędów, które były do tego zobowiązane). Było to niezgodne z art. 19b ust. 3 ustawy o informatyzacji [str. 32–33].
- **Większość z badanych systemów informatycznych (72 z 77) współpracowało z innymi systemami informatycznymi kontrolowanych urzędów, jednak tylko dwanaście z nich (16,7%) zapewniało współpracę na poziomie najbardziej dojrzałym, tj. transakcyjnym, co oznacza, że przekazywanie danych odbywało się w sposób w pełni zautomatyzowany.** Zaznaczyć należy, że tylko pięć systemów informatycznych (6,9%) bezpośrednio korzystało z danych gromadzonych w zewnętrznych systemach/rejestrach publicznych (zasada referencji), takich jak rejestr centralny PESEL czy też System Informacji Przestrzennej. Pozostałe badane systemy informatyczne korzystały wyłącznie z wewnętrznych zbiorów danych urzędów [str. 34–35].

2.2.3. Zarządzanie bezpieczeństwem systemów informatycznych w urzędach gmin miejskich i miast na prawach powiatu

- **W 15 urzędach, tj. 62,5% objętych kontrolą nie opracowano i nie wdrożono Polityki Bezpieczeństwa Informacji (dalej PBI), która jest elementem systemu zarządzania bezpieczeństwem informacji.** Przepis § 20 ust. 1 rozporządzenia KRI zobowiązuje podmioty realizujące zadania publiczne m.in. do opracowania, ustanowienia, wdrożenia, monitorowania i dokonywania przeglądów systemu zarządzania bezpieczeństwem informacji. W myśl § 20 ust. 3 tego rozporządzenia wymagania w zakresie systemu zarządzania bezpieczeństwem informacji uznaje się za spełnione, jeżeli system ten został opracowany na podstawie Polskich Norm[27]. W pkt 5.1 normy PN-ISO/IEC 17799:2007 wskazano opracowanie i stosowanie dokumentu polityki bezpieczeństwa informacji. Wdrożone w tych jednostkach procedury dotyczyły głównie zarządzania bezpieczeństwem danych osobowych, nie odnosiły się natomiast

[24] Paragraf 8 rozporządzenia ePUAP z 6 maja 2014 r., obowiązującego od 11 maja 2014 r. Poprzednio określone w § 7 ust. 1 rozporządzenia ePUAP z 27 kwietnia 2011 r.

[25] UM w: Mińsku Mazowieckim i Płocku.

[26] UM w: Andrychowie, Głogowie, Luboniu, Nowym Targu, Płocku, Radomiu i Śremie.

[27] Polska Norma PN-ISO/IEC 27001:2007 *Technika informatyczna. Techniki bezpieczeństwa. Systemy zarządzania bezpieczeństwem informacji. Wymagania* oraz powiązana z nią Polska Norma PN-ISO/IEC 17799:2007 *Technika informatyczna. Techniki bezpieczeństwa. Praktyczne zasady zarządzania bezpieczeństwem informacji.*

do innych informacji przetwarzanych w urzędzie[28]. Kontrolowani informowali, że planowane są, bądź podjęto już prace dla przygotowania nowej Polityki Bezpieczeństwa Informacji, która obejmie wszystkie elementy systemu zarządzania bezpieczeństwem informacji w urzędzie [str. 36–37].

- **W zdecydowanej większości jednostek (22 z 24, tj. 91,7%) w okresie objętym kontrolą przeprowadzano okresowe analizy utraty integralności, poufności lub dostępności informacji.** W analizach zidentyfikowano m.in. ryzyka braku ciągłości pracy jednostki, a także dla każdego ryzyka określano planowane działania mające na celu jego ograniczenie oraz koszty tych działań [str. 37–38].
- **W czterech urzędach[29] z 23[30] urzędów (tj. 17,4%) nie prowadzono inwentaryzacji zasobów informatycznych, w sposób określony w § 20 ust. 2 pkt 2 rozporządzenia KRI.** Dane sprzętu komputerowego ujmowano w układzie kart informacyjnych lub tradycyjnej książki inwentarzowej dla potrzeb rachunkowości. Nie zawierały one jednak szczegółowych danych o konfiguracji technicznej urządzeń, czy też o zainstalowanym na nich oprogramowaniu. Zdaniem NIK, prowadzenie inwentaryzacji zawierającej dane szczegółowe o konfiguracji technicznej urządzeń oraz o zainstalowanym na nich oprogramowaniu może ułatwić sprawne odtworzenie zasobów informatycznych w razie wystąpienia zdarzeń losowych jak np. kradzież lub poważna awaria sprzętu informatycznego. Ponadto, w dwóch innych urzędach[31] inwentaryzację zasobów informatycznych prowadzono w sposób nierzetelny [str. 38].
- **Nie opracowano pisemnych procedur zarządzania uprawnieniami użytkowników do pracy w systemach informatycznych w jednym urzędzie[32], a w 13 innych urzędach[33] (54,2%) stwierdzono nieprawidłowości polegające na niedochowaniu wymogów określonych w § 20 ust. 2 pkt 4 i 5 rozporządzenia KRI.** I tak:
  - w przypadku 18 osób (z 421 pracowników objętych badaniem) stwierdzono, że wystąpiły nieprawidłowości w zakresie nadawania uprawnień do realizowanych zadań [str. 39];
  - konta w systemach informatycznych 20 byłych pracowników (z 310 objętych badaniem) nie zostały zablokowane i pozostawały wciąż aktywne [str. 39];
  - w przypadku 82 pracowników wykonujących zadania w systemach informatycznych (z 350 objętych badaniem) stwierdzono, że mieli oni możliwość zainstalowania na użytkowanych przez nich komputerach dowolnego oprogramowania. Sytuacja taka wystąpiła w dziewięciu urzędach[34] (37,5%), a w czterech[35] z nich wszyscy badani użytkownicy systemów informatycznych niebędący pracownikami służb informatycznych posiadali uprawnienia administratora systemu, w związku z czym mogli samodzielnie instalować dowolne oprogramowanie [str. 40].

---

28 M.in. dotyczących konfiguracji infrastruktury informatycznej, w tym serwerów, zarządzania hasłami dostępu do systemów informatycznych, treści umów z dostawcami, warunków zastrzeżonych przez dostawców, tajemnic wynikających z innych aktów prawnych, jak np. prawa własności intelektualnej, zasad bezpieczeństwa fizycznego w obiekcie, korespondencji służbowej czy stosowanych zabezpieczeń systemów informatycznych.

29 Dotyczy UM w: Nowym Targu, Olkuszu, Pruszkowie i Świnoujściu.

30 Badania nie przeprowadzono w Urzędzie Miasta Płocka ze względu na trwającą w trakcie kontroli migrację danych do nowo zakupionego programu inwentaryzacyjnego.

31 UM w: Głogowie i Mińsku Mazowieckim.

32 UM w Stargardzie Szczecińskim.

33 UM w: Chrzanowie, Dzierżoniowie, Głogowie, Lesznie, Luboniu, Mikołowie, Mińsku Mazowieckim, Nowym Targu, Olkuszu, Płocku, Pruszkowie, Szczecinku i Świnoujściu.

34 UM w: Chrzanowie, Głogowie, Luboniu, Mińsku Mazowieckim, Nowym Targu, Olkuszu, Pruszkowie, Szczecinku i Świnoujściu.

35 UM w: Luboniu, Mińsku Mazowieckim, Nowym Targu i Świnoujściu.

- **W 17 urzędach (70,8%) zorganizowano dla pracowników szkolenia dotyczące bezpieczeństwa informacji, zgodnie z § 20 ust. 2 pkt 6 rozporządzenia KRI.** W pozostałych siedmiu jednostkach[36] po 31 maja 2012 r., tj. po wejściu w życie rozporządzenia KRI, nie przeprowadzono szkoleń w zakresie bezpieczeństwa informacji. Zdaniem NIK istnieje potrzeba, aby pracownicy zaangażowani w proces przetwarzania informacji zostali przeszkoleni oraz aby byli regularnie powiadamiani o zagrożeniach w obszarze bezpieczeństwa informacji, a także o zmianach w zakresie obowiązujących w urzędzie polityk i procedur związanych z wykonywanymi przez nich zadaniami. Zwiększy to świadomość pracowników co do występujących zagrożeń związanych z bezpieczeństwem informacji [str. 40–41].
- **Zasady bezpiecznej pracy użytkowników przy wykorzystaniu komputerów przenośnych zgodne z wymogami określonymi w § 20 ust. 2 pkt 8 rozporządzenia KRI ustanowiono tylko w 11 urzędach[37] (45,8%).** Zasady określały m.in. sposoby zabezpieczenia urządzeń mobilnych (laptopy, tablety, smartfony) i danych w nich zawartych przed kradzieżą i nieuprawnionym dostępem poza siedzibą jednostki, a także zasady korzystania z ogólnodostępnych sieci bezprzewodowych oraz aktualizacji oprogramowania urządzeń przenośnych [str. 41–42].
- **W ośmiu skontrolowanych urzędach (33,3%) w umowach na zakup lub serwis sprzętu komputerowego/oprogramowania dotyczących badanych systemów informatycznych, brak było zapisów gwarantujących zabezpieczenie poufności informacji uzyskanych przez wykonawców w związku z realizacją tych umów, co było niezgodne z przepisem § 20 ust. 2 pkt 10 rozporządzenia KRI.** Zapisów takich nie zawarto w 28[38] umowach spośród 63 umów objętych badaniem (44,4%). Wskazywane przez kontrolowanych „uzgodnienia nieformalne" bez wprowadzenia odpowiednich zapisów w umowach, zdaniem NIK mogą istotnie utrudniać zamawiającemu skuteczne dochodzenie odpowiedzialności usługodawcy w przypadku niedochowania tajemnicy informacji, do jakich miał on dostęp w związku z realizowaniem umowy [str. 42–43].
- **W dziewięciu[39] urzędach (tj. 37,5%) w okresie objętym kontrolą nie przeprowadzono audytu w zakresie bezpieczeństwa informacji w systemach informatycznych, co było niezgodne z § 20 ust. 2 pkt 14 rozporządzenia KRI.** Powyższą nieprawidłowość tłumaczono m.in. faktem, że audyt o podobnej tematyce został przeprowadzony w latach wcześniejszych, a także brakiem pracowników posiadających niezbędną wiedzę i doświadczenia dla przeprowadzenia takiego audytu[40] [str. 43–44].
- **W 20 kontrolowanych urzędach (83,3%) kopie zapasowe danych były właściwie tworzone, przechowywane oraz testowane.** Jednakże w czterech urzędach[41] stwierdzono nieprawidłowości w tym zakresie, stanowiące naruszenie § 20 ust. 2 pkt 12 lit. b rozporządzenia KRI [str. 44].

36 UM w: Chrzanowie, Dzierżoniowie, Luboniu, Nowym Targu, Olkuszu, Szczecinku i Świnoujściu.

37 UM w: Dąbrowie Górniczej, Legnicy, Lesznie, Luboniu, Mysłowicach, Ostrowie Wlkp., Płocku, Radomiu, Szczecinku, Świdnicy i Zawierciu.

38 UM w (liczba umów bez właściwych zapisów/liczba zbadanych umów): Dzierżoniowie (3/6), Głogowie (4/13), Lesznie (1/1), Nowym Targu (2/6), Olkuszu (5/22), Pruszkowie (4/4), Śremie (4/4) i Świnoujściu (5/7).

39 UM w: Andrychowie, Głogowie, Lesznie, Olkuszu, Pruszkowie, Stargardzie Szczecińskim, Szczecinku, Świnoujściu i Zawierciu.

40 W trakcie kontroli bądź w odpowiedziach na wystąpienia pokontrolne, kontrolowani zadeklarowali przeprowadzenie audytu bezpieczeństwa informacji w ostatnim kwartale 2014 r.

41 Dotyczy UM w: Luboniu, Mińsku Mazowieckim, Nowym Targu, Pruszkowie.

2.2.4. Dostosowanie sposobu prezentacji informacji przez systemy informatyczne do potrzeb osób niepełnosprawnych

- **Strony internetowe i BIP skontrolowanych urzędów w różnym stopniu zostały dostosowane do odbioru ich treści przez osoby niepełnosprawne.** W urzędach stosowano różne rozwiązania techniczne umożliwiające osobom niedosłyszącym lub niedowidzącym zapoznanie się z treścią informacji m.in. poprzez powiększenie czcionki, obrazu, zmianę kontrastu czy też odsłuchanie wyświetlanej treści. Ustalono, że we wszystkich kontrolowanych urzędach na ich stronach internetowych i/lub na stronach BIP występowały jednak błędy związane z prezentowaniem treści dla osób niepełnosprawnych. Niezbędne jest więc podejmowanie dalszych działań w celu wyeliminowania ujawnionych błędów i poprawy funkcjonalności stron internetowych i BIP w odbiorze przez osoby niepełnosprawne. Biorąc pod uwagę, że wymagania w tym zakresie określone w § 19 rozporządzenia KRI mają być ostatecznie wprowadzone nie później niż w terminie 3 lat od dnia wejścia w życie rozporządzenia KRI, tj. do dnia 31 maja 2015 r., NIK nie dokonywała oceny działalności kontrolowanych jednostek w badanym obszarze [str. 45].

2.3 Uwagi i wnioski

1. Wyniki kontroli wskazują, że jakkolwiek podjęte zostały działania dla zapewnienia interoperacyjności zakupionych i zmodernizowanych po 31 maja 2012 r. systemów informatycznych, to jednak zakres tej współpracy jest jeszcze ograniczony. Świadczy o tym to, iż zaledwie 16,7% z badanych systemów informatycznych automatycznie wymieniało informacje z innymi systemami urzędu, jak również fakt, że tylko 6,9% systemów odwoływało się bezpośrednio do danych gromadzonych w zewnętrznych systemach/rejestrach publicznych. Konieczne jest zatem podejmowanie przez MAiC i podmioty realizujące zadania publiczne dalszych działań w celu osiągnięcia wyższego poziomu interoperacyjności systemów informatycznych. Jest to bowiem jeden z głównych elementów, który tworzy warunki dla rozwoju rynku usług świadczonych drogą elektroniczną obywatelom i przedsiębiorcom, na co wskazano w Programie Zintegrowanej Informatyzacji Państwa. Wyniki kontroli wykazały, że liczba świadczonych usług elektronicznych w większości kontrolowanych urzędów (70,8%) nie przekraczała 20, a w czterech urzędach ograniczała się do świadczenia tylko jednej, obligatoryjnej usługi, tj. Elektronicznej Skrzynki Podawczej.
2. Dla rozwoju usług elektronicznych istotne jest również pełne i konsekwentne wprowadzenie w urzędach elektronicznego systemu zarządzania dokumentacją, który – jak wskazują wyniki kontroli – stosowany jest bardziej jako element pomocniczy dla papierowego systemu dokumentowania przebiegu rozpatrywania i rozstrzygania spraw.
3. W celu większego zainteresowania obywateli i przedsiębiorców możliwością załatwiania spraw w urzędzie drogą elektroniczną, istnieje potrzeba podjęcia szerszych działań w zakresie informowania o e-usługach i ich promowania, w szczególności tam, gdzie urzędy świadczą wiele usług w formie elektronicznej, ale liczba złożonych dokumentów w tej formie jest znikoma. W trakcie kontroli stwierdzono, że niektóre urzędy podejmowały aktywne działania w zakresie informowania i promowania komunikacji elektronicznej z urzędem, co należy wskazać jako tzw. dobre praktyki. Polegały one np. na organizowaniu spotkań z mieszkańcami, przeprowadzaniu ankiet, a także zamieszczaniu stosownych informacji w lokalnych mediach.

4. W komunikacji urzędu z osobami niepełnosprawnymi istotnego znaczenia nabiera również kwestia właściwego prezentowania informacji poprzez właściwe dostosowanie dla tych osób treści zamieszczanych na stronach internetowych i BIP urzędów. Kontrola wykazała, że w żadnym z kontrolowanych urzędów do zakończenia kontroli jeszcze nie dostosowano w pełni serwisów internetowych do wymagań określonych w § 19 rozporządzenia KRI, które wejdą w życie 31 maja 2015 r.
5. Dla zapewnienia prawidłowej i bezpiecznej komunikacji drogą elektroniczną wewnątrz urzędu jak i z innymi urzędami oraz z obywatelami istotnym jest zapewnienie bezpieczeństwa informacji. Służyć temu powinien prawidłowo funkcjonujący system zarządzania bezpieczeństwem informacji, w szczególności przyjęcie i konsekwentne wdrożenie oraz stosowanie polityki bezpieczeństwa informacji. Tymczasem kontrola NIK wykazała, że w tym obszarze wystąpiło wiele nieprawidłowości polegających na niedochowaniu wymogów określonych w § 20 rozporządzenia KRI.
6. Ważną rolę w zarządzaniu osiąganiem interoperacyjności systemów informatycznych ma do spełnienia Minister Administracji i Cyfryzacji, który w tym zakresie realizuje zadania określone w ustawie o informatyzacji i rozporządzeniu KRI. Obejmują one m.in. koordynowanie spraw w zakresie opracowywania standardów, wytycznych i rekomendacji interoperacyjności oraz prowadzenie kontroli w podmiotach publicznych w zakresie działania systemów teleinformatycznych, prowadzenia rejestrów i wymiany informacji w postaci elektronicznej, przewidzianych w art. 25 ust. 1 pkt 3 lit. c ustawy o informatyzacji. Kontrole takie przez MAiC nie były prowadzone. Ponadto, nie przekazano wojewodom jednolitych kryteriów merytorycznych dotyczących przeprowadzania przez nich kontroli w jednostkach samorządu terytorialnego w zakresie działania systemów teleinformatycznych oraz rejestrów publicznych, które są używane do realizacji zadań zleconych z zakresu administracji rządowej. Zdaniem NIK, prowadzenie takich kontroli zarówno przez MAiC, jak i wojewodów, jest niezbędne gdyż zapewnia wiedzę o praktycznym funkcjonowaniu systemów informatycznych w podmiotach podlegających wymogom rozporządzenia KRI.

* * *

W ocenie NIK, dla zwiększenia poziomu interoperacyjności systemów informatycznych oraz bezpieczeństwa przetwarzanych w nich danych konieczne jest podejmowanie przez Ministra Administracji i Cyfryzacji i jednostki samorządu terytorialnego działań, w szczególności:

Minister Administracji i Cyfryzacji powinien:

- Zapewnić przeprowadzanie przewidzianych w art. 25 ust. 1 pkt 3 lit. c ustawy o informatyzacji kontroli w podmiotach publicznych w zakresie działania systemów teleinformatycznych, prowadzenia rejestrów i wymiany informacji w postaci elektronicznej.
- Podjąć działania w celu doprecyzowania podmiotom realizującym zadania publiczne znaczenia terminu „istotnej modernizacji", o której mowa w § 23 rozporządzenia KRI.
- Określić dla wojewodów jednolite i spójne kryteria kontroli systemów/rejestrów informatycznych używanych w jednostkach samorządu terytorialnego do realizacji zadań zleconych z zakresu administracji rządowej (art. 25 ust. 1 pkt 3 lit. a ustawy o informatyzacji).

Burmistrzowie i Prezydenci miast powinni:

- Przeprowadzać, przy zakupie nowych lub modernizacji już funkcjonujących systemów informatycznych, analizy zapewnienia interoperacyjności (współdziałania) z innymi systemami w celu optymalnego wykorzystywania danych już zgromadzonych we własnych i zewnętrznych systemach/rejestrach informatycznych.
- Rozważyć możliwość wprowadzenia systemu elektronicznego zarządzania dokumentacją jako podstawowego sposobu dokumentowania przebiegu załatwiania i rozstrzygania spraw.
- Opracować i wdrożyć PBI oraz konsekwentnie stosować procedury zarządzania bezpieczeństwem informacji przetwarzanych w urzędzie, obejmujące wszystkie elementy, o których mowa w § 20 rozporządzenia KRI.
- Podjąć lub zintensyfikować działania informacyjne i promocyjne w celu zachęcenia obywateli i przedsiębiorców do korzystania z elektronicznej formy komunikacji z urzędem.
- Zapewnić do 31 maja 2015 r. dostosowanie prezentowanych informacji w systemach teleinformatycznych urzędów, w tym na stronach internetowych i BIP do odbioru przez osoby niepełnosprawne, stosownie do wymagań określonych w § 19 rozporządzenia KRI.

3 WAŻNIEJSZE WYNIKI KONTROLI

3.1 Realizacja zadań Ministra Administracji i Cyfryzacji w zakresie interoperacyjności, w szczególności określonych w rozporządzeniu KRI, w zakresie prowadzenia repozytorium interoperacyjności oraz publicznej dyskusji nad rekomendacjami interoperacyjności.

Minister Administracji i Cyfryzacji zgodnie z § 9 rozporządzenia KRI, zapewnia realizację publicznej dyskusji nad rekomendacjami interoperacyjności (pkt 1) oraz prowadzenie repozytorium interoperacyjności (pkt 2).

3.1.1. Rekomendacje interoperacyjności

Zadania Ministra Administracji i Cyfryzacji w zakresie m.in. przygotowywania rekomendacji dotyczących interoperacyjności, neutralności technologicznej i jawności standardów informatycznych dla systemów teleinformatycznych używanych do realizacji zadań publicznych, rekomendowania strategicznych zadań państwa, standardów i wytycznych w zakresie informatyzacji administracji publicznej, przygotowywania rekomendacji dotyczących minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej z podmiotami publicznymi, zgodnie z Regulaminem organizacyjnym MAiC[42], wykonywał Departament Informatyzacji (dalej *DI*).

Minister Administracji i Cyfryzacji w okresie objętym kontrolą zapewnił prowadzenie publicznej dyskusji nad rekomendacjami interoperacyjności na Portalu Interoperacyjności zamieszczonym na ePUAP[43]. Portal Interoperacyjności (dalej *PI*) stanowi narzędzie, przy wykorzystaniu którego Minister organizuje publiczną dyskusję w zakresie wypracowania rekomendacji i wzorców stosowanych przy świadczeniu usług publicznych. Ponadto, Z-ca Dyrektora DI podała, iż (…) *w ramach obecnie realizowanego przez Ministerstwo Administracji i Cyfryzacji, we współpracy z Centrum Projektów Informatycznych, projektu ePUAP rozbudowywane są funkcjonalności systemu ePUAP, po zakończeniu którego udostępniona zostanie nowa wersja platformy, w tym nowe funkcjonalności w zakresie repozytorium interoperacyjności.*

Do dnia zakończenia czynności kontrolnych w MAiC[44] na PI zamieszczone były informacje dotyczące prowadzonych dyskusji w zakresie interoperacyjności w ramach 33 wątków[45], w tym pięć utworzonych w okresie objętym kontrolą. W szczególności istotne dla zagadnień objętych kontrolą były dwa wątki[46] udostępnione przez Ministra Administracji i Cyfryzacji wraz ze wstępnymi propozycjami w związku z nowelizacją ustawy o informatyzacji w celu przeprowadzenia dyskusji i wypracowania właściwego rozwiązania dla:

- Standardu Elektronicznej Skrzynki Podawczej – opisu niezbędnych właściwości, jakie powinna posiadać ESP udostępniana przez podmioty publiczne;
- Standardu Formularza ePUAP – opisu charakterystycznych elementów, jakie powinien lub może posiadać formularz używany przez podmioty publiczne na platformie ePUAP, wraz załącznikiem do Standardu, w którym zawarto opis podstawowych elementów Formularza (formularz.xsd[47]), stanowiącego podstawę do jednego ze sposobów weryfikacji Formularzy instalowanych na ePUAP.

---

42 W okresie objętym kontrolą obowiązywały dwa regulaminy organizacyjne wprowadzone zarządzeniami Ministra Administracji i Cyfryzacji w sprawie ustalenia regulaminu organizacyjnego Ministerstwa Administracji i Cyfryzacji: nr 5 z dnia 27 grudnia 2011 r. – obowiązywał do 21 stycznia 2013 r. (Dz. Urz. MAiC z 2012 r., poz. 5) oraz nr 1 z dnia 15 stycznia 2013 r. – obowiązywał od dnia 22 stycznia 2013 r. (Dz. Urz. MAiC z 2013 r., poz. 1).

43 PI został udostępniony na ePUAP w następującej lokalizacji: strona główna www.epuap.gov.pl>Podmioty publiczne>Portal Interoperacyjności.

44 Tj. do dnia 14 lipca 2014 r.

45 Wątek stanowi pewną przestrzeń roboczą na Portalu Interoperacyjności, w ramach której trwają prace nad rekomendacją.

46 Pozostałe trzy wątki to: *Dziedzinowe schematy dla MF – aktualizacja; Wzory załączników ogólnych; Wzory załączników – VAT.*

47 XSD – jest plikiem schematu dla wzoru określającego strukturę dokumentu elektronicznego w formacie xml.

3.1.2. Repozytorium interoperacyjności

Minister Administracji i Cyfryzacji zapewnił prowadzenie repozytorium interoperacyjności[48]. W RI zamieszczono informację o 26 rekomendacjach interoperacyjności[49], o których mowa w § 6 rozporządzenia KRI, w tym o rekomendacjach dotyczących standardu ESP oraz standardu Formularza ePUAP. W RI znajdowało się również 151 dokumentów[50], będących produktami tych rekomendacji[51].

Zgodnie z § 7 ust. 1 rozporządzenia KRI informacje opublikowane w repozytorium interoperacyjności powinny być oznaczone w szczególności: nazwą, opisem, wersją, datą i czasem publikacji, statusem obowiązywania, identyfikatorem pozwalającym na identyfikację osoby publikującej. Szczegółowe badanie przeprowadzone na próbie dokumentów zamieszczonych w RI wykazało, że były one oznaczone w sposób określony w tym przepisie.

Minister Administracji i Cyfryzacji, stosownie do § 10 ust. 5 rozporządzenia KRI, opublikował w RI schematy XML struktury danych cech informacyjnych obiektów. Jest to standard wymiany plików używany w komunikacji między systemami informatycznymi, przyjęty do stosowania w administracji publicznej. Schematy te odnosiły się do:

- osób fizycznych posiadających nadany numer PESEL,
- osób prawnych, jednostek organizacyjnych nie posiadających osobowości prawnej oraz organów władzy publicznej,
- obiektów przestrzennych[52].

W RI nie publikowano schematów XML struktur danych cech informacyjnych innych typów obiektów niż powyższe, ponieważ podmioty publiczne w okresie objętym kontrolą nie składały do MAiC wniosków, o których mowa w § 10 ust. 12 rozporządzenia KRI. Z powodu braku wniosków podmiotów publicznych nie publikowano również opisów protokołów i struktur wymiany danych usługi sieciowej, o których mowa w § 8 ust. 3 tego rozporządzenia.

3.1.3. Działania informacyjne w zakresie KRI

W związku z wejściem w życie rozporządzenia KRI, pracownicy Departamentu Informatyzacji MAiC przeprowadzali szkolenia dotyczące interoperacyjności, m.in. w maju 2014 r. na prośbę Departamentu Rozwoju Cyfrowego Ministerstwa Infrastruktury i Rozwoju, przeprowadzone zostały warsztaty poświęcone interoperacyjności systemów teleinformatycznych adresowane do pracowników instytucji zaangażowanych we wdrażanie Programu Operacyjnego Polska Cyfrowa oraz potencjalnych beneficjentów i przedstawicieli Urzędów Marszałkowskich odpowiedzialnych za przygotowanie Regionalnych Programów Operacyjnych. Na spotkaniach i konferencjach pracownicy Departamentu Informatyzacji omawiali zagadnienia związane z interoperacyjnością, np. w dniu 22 maja 2013 r. na spotkaniu audytorów wewnętrznych jednostek sektora finansów publicznych[53], w czerwcu 2013 r. na konferencji pn. „E-dostępność sektora publicznego w Polsce

[48] Repozytorium interoperacyjności zostało udostępnione na stronie internetowej www.crd.gov.pl>„Podmioty publiczne”>„PI”>„Produkty Rekomendacji”.

[49] Rekomendacja to dokument wypracowany w ramach Portalu Interoperacyjności. W ramach jednej rekomendacji mogą powstać różne produkty (np. schemat XML).

[50] Pojedynczy, podstawowy lub złożony składnik wzoru dokumentu elektronicznego lub inny dokument np. standard.

[51] Efekt przeprowadzonej dyskusji, wypracowane rozwiązanie.

[52] Element świata rzeczywistego przyjęty w układzie współrzędnych np. budynek o ustalonym adresie.

[53] http://www.mf.gov.pl/news1/-/asset_publisher/u7QN/content/id/4581781;jsessionid=DAA4E860D38EC36400930548DD4823AB

– osiągnięcia i wyzwania"[54]. Jak podała Dyrektor Generalny MAiC, temat interoperacyjności omawiany był także na spotkaniach Linii Współpracy[55] strony rządowej z samorządową, w ramach grupy roboczej ds. elektronizacji[56]. Ponadto, w 2013 r. organizowane były w MAiC spotkania pod przewodnictwem Podsekretarza Stanu Pana Andrzeja Ręgowskiego, mające na celu wypracowanie rozwiązań w zakresie interoperacyjności rejestrów publicznych. W ramach cyklu ww. spotkań wypracowano wykaz krytycznych cech informacyjnych dla rejestrów publicznych oraz opracowano i przetestowano narzędzie analityczne dotyczące budowy modelu współdziałania usług z rejestrami publicznymi.

NIK pozytywnie oceniła podejmowane przez MAiC działania mające na celu zapoznanie przedstawicieli administracji publicznej z zagadnieniami interoperacyjności systemów informatycznych.

Po wejściu w życie rozporządzenia KRI, różne podmioty[57] zwracały się do MAiC o udzielenie informacji i wyjaśnień w sprawach regulowanych ww. rozporządzeniem. Ministerstwo na bieżąco udzielało odpowiedzi na zgłoszone pytania i wątpliwości, za wyjątkiem jednego przypadku:

- *Ustalono, iż Wojewoda Podlaski w uzgodnieniu z pozostałymi wojewodami, w dniu 17 lipca 2012 r. skierował do Ministra Administracji i Cyfryzacji pismo (znak: BI-I.002.1.2012.MS) z prośbą o wyjaśnienie sposobu realizacji obowiązku określonego w art. 25 ust. 1 pkt 3 lit. a ustawy o informatyzacji, dotyczącego przeprowadzania kontroli w jednostkach samorządu terytorialnego w zakresie działania systemów teleinformatycznych oraz rejestrów publicznych, które są używane do realizacji zadań zleconych z zakresu administracji rządowej. Wojewoda Podlaski w ww. piśmie przedstawił najistotniejsze problemy w zakresie realizacji przedmiotowej kontroli oraz zwrócił się z prośbą o określenie jednolitych kryteriów merytorycznych kontroli. W toku kontroli ustalono, iż ww. pismo wpłynęło do MAiC w dniu 25 lipca 2012 r. i do dnia zakończenia kontroli, tj. do dnia 14 lipca 2014 r. nie została udzielona na nie odpowiedź, a MAiC w udzielonych wyjaśnieniach nie wskazał na przyczynę braku odpowiedzi.*

  NIK wskazała, że brak odpowiedzi może utrudniać wywiązywanie się przez wojewodów z obowiązku przeprowadzania kontroli dotyczących stosowania przepisów rozporządzenia KRI. Z uzyskanych przez NIK informacji wynika, iż 14 wojewodów nie przeprowadzało kontroli w jednostkach samorządu terytorialnego w zakresie działania systemów teleinformatycznych oraz rejestrów publicznych, które są używane do realizacji zadań zleconych z zakresu administracji rządowej[58].

Najwięcej wątpliwości podmioty zgłaszały w sprawach dotyczących przeprowadzania audytu w zakresie bezpieczeństwa informacji i znaczenia terminu „istotnej modernizacji". W ocenie NIK, pozytywnie należy ocenić opracowanie przez Departament Informatyzacji MAiC w uzgodnieniu z Departamentem Audytu Sektora Finansów Publicznych Ministerstwa Finansów wspólnego stanowiska odnośnie zagadnień związanych z obowiązkiem przeprowadzania okresowego audytu w zakresie bezpieczeństwa informacji, o którym mowa w § 20 ust. 2 pkt 14 rozporządzenia KRI. Powyższe stanowisko wraz z wytycznymi do przeprowadzenia audytu zostało zamieszczone na stronie internetowej Ministerstwa Finansów.

54 http://widzialni.org/e-dostepnosc-sektora-publicznego-w-polsce-osiagniecia-i-wyzwania,m,mg,8,27

55 Linia Współpracy to sposób współpracy między samorządami i rządem. Pozwala samorządowcom i administracji rządowej konsultować założenie projektów teleinformatycznych na wczesnym etapie. Ponieważ projekty są różne, powstały cztery grupy robocze, które spotykają się cyklicznie i specjalizują w: elektronizacji usług administracji, e-umiejętnościach i partycypacji cyfrowej, sprawach otwartego rządu, budowie sieci szerokopasmowych budowanych ze środków unijnych (źródło: https://mac.gov.pl/linia-wspolpracy-rzadu-i-samorzadu).

56 http://maic.gov.pl/grupa-ds-elektronizacji-uslug-administracji

57 Polski Związek Niewidomych, firma Librus, Urząd Miasta i Gminy w Gryfinie, Urząd Miasta i Gminy Uzdrowiskowej Muszyna, Ministerstwo Finansów – Departament Audytu Sektora Finansów Publicznych.

58 NIK zwróciła się, na podstawie art. 29 ust. 1 pkt 2 lit. f ustawy o NIK do wszystkich wojewodów o udzielenie informacji dotyczących kontroli jednostek samorządu terytorialnego przeprowadzanych na podstawie art. 25 ust. 1 pkt 3 lit a w związku z art. 25 ust. 3 ustawy o informatyzacji, tj. w zakresie działania systemów teleinformatycznych oraz rejestrów publicznych, które są używane do realizacji zadań zleconych z zakresu administracji rządowej.

Natomiast w kwestii rozumienia terminu „istotnej modernizacji", o którym mowa w § 23 rozporządzenia KRI Zastępca Dyrektora DI poinformowała, że do oceny jaka modernizacja jest istotna, właściwy jest administrator konkretnego zmodernizowanego systemu informatycznego. Poinformowała również, że ocena taka zawsze będzie indywidualna oraz uzależniona od specyfiki konkretnego systemu, niemniej jednak kryteria w oparciu, o które przedmiotowa ocena powinna być dokonywana to w szczególności zmiana funkcjonalności, używalności, wydajności lub niezawodności systemu czy też nakład czasowy związany ze zmianą oraz nakład finansowy niezbędny do przeprowadzenia modernizacji. NIK zauważa, że w trakcie prac legislacyjnych nad projektem rozporządzenia KRI Podsekretarz Stanu w MSWiA Pan Piotr Kołodziejczyk w piśmie z dnia 10 sierpnia 2011 r. nr DSI-WPISI-0230-9-1/2011 przedstawił wyjaśnienie, że „Poprzez istotną modernizację należy rozumieć modernizację co najmniej na poziomie 10% ogólnej wartości systemu".

W opinii NIK, brak precyzyjnego określenia pojęcia „istotnej modernizacji" może utrudniać interpretację tego pojęcia przez podmioty realizujące zadania publiczne. Ma to znaczenie w aspekcie realizacji obowiązku określonego w § 23 rozporządzenia KRI, który zobowiązuje ww. podmioty do dostosowania użytkowanych systemów teleinformatycznych do wymogów zawartych w rozdziale IV rozporządzenia KRI, nie później niż w dniu ich pierwszej istotnej modernizacji.

3.1.4. Kontrola interoperacyjności systemów informatycznych w podmiotach publicznych

Zgodnie z art. 25 ust. 1 pkt 3 lit. c ustawy o informatyzacji, minister właściwy do spraw informatyzacji dokonuje kontroli w podmiotach publicznych[59] działania systemów teleinformatycznych, używanych do realizacji zadań publicznych albo realizacji obowiązków wynikających z art. 13 ust. 2 ww. ustawy – pod względem zgodności z minimalnymi wymaganiami dla systemów teleinformatycznych lub minimalnymi wymaganiami dla rejestrów publicznych i wymiany informacji w postaci elektronicznej.

Zadania kontrolne w MAiC przypisane były[60] do zakresu działania Departamentu Kontroli, Skarg i Wniosków (dalej *DKSiW*). W okresie objętym kontrolą DKSiW nie planował i nie przeprowadzał kontroli w wyżej wymienionym zakresie. Natomiast na podstawie upoważnienia udzielonego przez Prezesa Rady Ministrów, DKSiW przeprowadził w okresie od 17 czerwca 2013 r. do 31 maja 2014 r. kontrolę projektu ponadsektorowego[61] pn.: *Elektroniczna Platforma Usług Administracji Publicznej 2 (ePUAP2)*.

Jak podał Dyrektor DKSiW, w latach 2011–2013 członkowie kierownictwa i komórki organizacyjne Ministerstwa nie wnioskowały o umieszczenie w planie kontroli realizacji przez DKSiW kontroli w podmiotach publicznych w zakresie działania systemów teleinformatycznych, używanych do realizacji zadań publicznych albo realizacji obowiązków określonych w art. 13 ust. 2 ustawy o informatyzacji. Jednocześnie Dyrektor DKSiW wskazał, iż Departament Informatyzacji MAiC weryfikuje zapewnienie interoperacyjności systemów teleinformatycznych na etapie prac nad projektami dokumentów rządowych rozpatrywanych przez Komitet Rady Ministrów ds. Cyfryzacji (dalej *KRMC*), za pomocą listy kontrolnej. Ponadto, wskazał, że pracownicy DKSiW

[59] Za wyjątkiem:
– jednostek samorządu terytorialnego i ich związków oraz w tworzonych lub prowadzonych przez te jednostki samorządowych osób prawnych i innych samorządowych jednostek organizacyjnych;
– podmiotów publicznych podległych lub nadzorowanych przez organy administracji rządowej.

[60] Zgodnie z § 22 Regulaminu organizacyjnego prowadzenie kontroli przypisane było do zakresu działania Departamentu Kontroli, Skarg i Wniosków.

[61] Zgodnie z art. 25 ust. 1 pkt 1 ustawy o informatyzacji, kontroli realizacji ponadsektorowych projektów informatycznych dokonuje Prezes Rady Ministrów.

nie spełniali wymogu określonego w art. 28 ust. 1 pkt 5 ustawy o informatyzacji, tj. nie posiadali certyfikatów wskazanych w rozporządzeniu Ministra Spraw Wewnętrznych i Administracji z dnia 10 września 2010 r. w sprawie wykazu certyfikatów uprawniających do prowadzenia kontroli projektów informatycznych i systemów teleinformatycznych[62]. Podejmowano starania mające na celu pozyskanie specjalistów posiadających certyfikat wskazany w tym rozporządzeniu. W wyniku tych starań w okresie od 17 czerwca 2013 r. do 30 kwietnia 2014 r. w DKSiW był zatrudniony ekspert, który jako członek zespołu kontrolnego uczestniczył w przygotowaniu i przeprowadzeniu kontroli projektu ponadsektorowego ePUAP2. Dalsze starania w opinii DKSiW o pozyskanie na stałe ekspertów do przeprowadzenia kontroli systemów informatycznych, nie były konieczne, ponieważ zarówno członkowie kierownictwa i komórki organizacyjne Ministerstwa nie wnioskowały o umieszczenie w planie kontroli określonych w art. 25 ust. 1 pkt 3 lit. c ustawy o informatyzacji.

Przedstawiona w powyższych wyjaśnieniach argumentacja nie uzasadniała, zdaniem NIK, niepodejmowania działań w celu realizacji przypisanych ustawowo Ministrowi Administracji i Cyfryzacji zadań kontrolnych. **Dla zapewnienia pełnego obrazu stanu osiąganej interoperacyjności systemów informatycznych w podmiotach publicznych niezbędnym jest prowadzenie kontroli w zakresie określonym w art. 25 ust. 1 pkt 3 lit. c ustawy o informatyzacji. W szczególności jest to konieczne z uwagi na dynamiczny przebieg procesu informatyzacji zachodzący aktualnie w kraju. Pozwoliłoby to również na wypracowanie rozwiązań możliwych do wykorzystania na etapie dokonywania ewentualnego przeglądu funkcjonowania wymogów określonych w rozporządzeniu KRI.**

Pan Bogdan Dombrowski Podsekretarz Stanu w Ministerstwie Administracji i Cyfryzacji w odpowiedzi na wystąpienie pokontrolne poinformował (z upoważnienia Ministra Administracji i Cyfryzacji) m.in., że skieruje pracownika na szkolenie/studia podyplomowe, kończące się uzyskaniem certyfikatu oraz że podjęto działania celem zatrudnienia osoby posiadającej wymagane kwalifikacje (certyfikaty). Podał również, że wzmocnienie DKSiW o pracowników spełniających dodatkowe kryterium określone w art. 28 ust. 1 pkt 5 ustawy o informatyzacji[63] pozwoli na prowadzenie kontroli w podmiotach publicznych w zakresie działania systemów teleinformatycznych, prowadzenia rejestrów i wymiany informacji w postaci elektronicznej.

3.1.5. Realizacja Programu Zintegrowanej Informatyzacji Państwa w obszarze interoperacyjności

W dniu 8 stycznia 2014 r. został przyjęty przez Radę Ministrów Program Zintegrowanej Informatyzacji Państwa opracowany przez MAiC we współpracy z pozostałymi resortami.

W punkcie 6.3.1. PZIP określone zostały zadania do zrealizowania w obszarze interoperacyjności, w tym zadania krótkookresowe, do zrealizowania w ciągu sześciu miesięcy od daty przyjęcia dokumentu, tj. do 8 lipca 2014 r.:

1) powołanie przez Komitet Rady Ministrów do spraw Cyfryzacji, międzyresortowego zespołu do spraw osiągania interoperacyjności mającego za zadanie koordynację przedsięwzięć z zakresu osiągania interoperacyjności,
2) opublikowanie schematów struktur danych cech informacyjnych podstawowych obiektów opisywanych w rejestrach publicznych,

[62] Dz. U. Nr 177, poz. 1195.

[63] Kontrolerem może być osoba pełnoletnia, która posiada certyfikat, uprawniający do prowadzenia kontroli projektów informatycznych i systemów teleinformatycznych w rozumieniu art. 25 ustawy o informatyzacji.

3) opublikowanie informacji o sposobie identyfikacji osób fizycznych nieposiadających numeru PESEL oraz podmiotów innych niż osoby fizyczne nieposiadających nadanego numeru REGON,
4) zidentyfikowanie rejestrów publicznych zawierających dane referencyjne niezbędne do realizacji procedur administracyjnych i uzyskanie od podmiotów publicznych prowadzących te rejestry zasad tworzenia identyfikatorów obiektów innych niż osoba, podmiot i obiekt przestrzenny oraz struktur danych cech informacyjnych.

Inicjowanie i koordynowanie działań administracji rządowej określonych w PZIP zostało powierzone Ministrowi Administracji i Cyfryzacji[64]. Zgodnie § 21 pkt 7 Regulaminu organizacyjnego MAiC, zadania związane z realizacją PZIP wykonywane były przez Departament Informatyzacji.

NIK zwróciła uwagę, że pomimo upływu terminu na wykonanie działań krótkoterminowych związanych z interoperacyjnością (określonych w PZIP), żadne z nich do dnia zakończenia kontroli NIK nie zostało w pełni zrealizowane. Wskazuje to na potrzebę przyspieszenia realizacji tych zadań, bowiem w ocenie NIK sytuacja taka stwarza zagrożenie opóźnienia realizacji pozostałych zadań określonych w tym programie w zakresie osiągania interoperacyjności systemów informacyjnych podmiotów realizujących zadania publiczne. Szczególną rolę w tym zakresie ma Minister Administracji i Cyfryzacji, któremu w PZIP powierzono inicjowanie i koordynowanie działań związanych z informatyzacją, a co za tym idzie, działania Ministra mają istotny wpływ na terminowość realizacji poszczególnych zadań programu.

Zastępca dyrektora DI, odpowiedzialna za zadania wynikające z PZIP podała, że ich realizacja będzie się odbywała przy współudziale podmiotów publicznych objętych zakresem regulacji wynikających z rozporządzenia KRI. Wskazała, iż *Przygotowane propozycje będą przedstawione Panu Ministrowi. (...) Kwestie interoperacyjności będą podlegały ocenie przy dokonywaniu oceny wniosków o dofinasowanie z PO PC, przy tym każdorazowo będą podlegały weryfikacji w zakresie uwzględnienia założeń i celów PZIP. Niezbędne do tego jest stworzenie mechanizmów współpracy pomiędzy MAiC, a innymi resortami, jednym z których powinien być zespół, o którym mowa w PZIP, działający przy KRMC. Trwają uzgodnienia z Komisją Europejską w zakresie merytorycznym dot. PO PC i jednocześnie trwają ustalenia pomiędzy MAiC, MIR a Władzą Wdrażającą w zakresie zarządzania PO PC. Chcemy, aby mechanizmy zarządzania dały możliwość realnego wpływu na finasowanie ze środków UE rozwiązań zapewniających m.in. interoperacyjność systemów w ramach systemu informacyjnego państwa.*

W zakresie realizacji pierwszego działania, z-ca dyrektora DI poinformowała, że (…) *określono główne obszary prac oraz propozycje składu międzyresortowego zespołu do spraw osiągania interoperacyjności mającego za zadanie koordynację przedsięwzięć z zakresu osiągania interoperacyjności.* Z ustaleń kontroli NIK wynika, że do dnia zakończenia czynności kontrolnych w MAiC, tj. do dnia 14 lipca 2014 r., zespół taki nie został powołany.

W zakresie działania drugiego, dotyczącego opublikowania schematów danych cech informacyjnych podstawowych obiektów opisywanych w rejestrach publicznych, jak poinformował Naczelnik Wydziału Polityki Informatyzacji Państwa w DI: *W 2008 r. opublikowano schematy podstawowych obiektów informacyjnych, tj. osoba fizyczna, podmiot, obiekt przestrzenny.*

Odnośnie działania trzeciego z-ca dyrektora DI wskazała, że właściwym do realizacji zadania opublikowania informacji o sposobie identyfikacji osób fizycznych nieposiadających numeru PESEL – jest MSW, a podmiotów innych niż osoby fizyczne nieposiadających nadanego numeru REGON – GUS.

64 Rozdział 7, str. 74 PZIP.

Naczelnik Wydziału Polityki Informatyzacji Państwa w DI właściwy w sprawach rejestrów wyjaśniając kwestię monitorowania realizacji tego zadania przez MAiC podał m.in., że rozpoczęto prace konsultacyjne w celu *(…) stworzenia innego jednoznacznego identyfikatora dla osoby fizycznej niż numer PESEL (…)*.

W zakresie działania czwartego, z-ca dyrektora DI podała, że w ramach organizowanych przez MAiC, cyklicznych spotkań dotyczących interoperacyjności z udziałem przedstawicieli podmiotów zewnętrznych, wykonane zostały prace w obszarze identyfikacji oraz analizy krytycznych cech informacyjnych dla rejestrów publicznych. Prace wykonywane w ramach tego działania nie zostały zakończone.

3.2 Działania burmistrzów i prezydentów miast w zakresie dostosowania posiadanych systemów informatycznych do współpracy z innymi systemami/rejestrami informatycznymi

3.2.1. Dokumenty strategiczne

W dokumentach strategicznych w większości z kontrolowanych urzędów (22[65] spośród 24, tj. 91,7%) uwzględniano problematykę związaną m.in. z takimi zadaniami i zagadnieniami jak:

- rozbudowa infrastruktury teleinformatycznej w celu upowszechnienia elektronicznego dostępu do urzędu,
- wykorzystanie nowoczesnych technologii w komunikacji mieszkańców z urzędem,
- usprawnienie funkcjonowania administracji samorządowej w ramach projektu e-urząd.

Określano też cele i zadania dotyczące rozwoju usług informatycznych. Na przykład:

- *W Strategii Rozwoju Społeczno-Gospodarczego dla Miasta Stargard Szczeciński do roku 2020 wskazano cel szczegółowy Podniesienie jakości usług w obiektach użyteczności publicznej, w ramach którego wyznaczono kierunek działania Informatyzacja oraz usprawnienie funkcjonowania administracji samorządowej w ramach projektu e-urząd. W opisie kierunku podano, że jego główną ideą jest w końcowym etapie jego realizacji doprowadzenie do pełnej możliwości obsługi petenta na drodze elektronicznej.*

3.2.2. Promowanie komunikacji elektronicznej

Tylko w 11[66] urzędach spośród 24 objętych badaniem (45,8%) podejmowano działania mające na celu promowanie komunikacji elektronicznej z urzędem, w tym możliwości korzystania z udostępnionych usług elektronicznych. Promocje takie były prowadzone poprzez zamieszczanie informacji o świadczonych usługach elektronicznych na stronach internetowych urzędów, w lokalnej telewizji i prasie, rozpowszechnianie materiałów reklamowych w formie ulotek i na lokalnych portalach internetowych.

Badania poznania potrzeb mieszkańców w zakresie korzystania z elektronicznych form komunikacji z urzędem wykazały, że zaledwie w kilku przypadkach[67] urzędy podejmowały związane z tym aktywne działania. Na przykład:

- *W **Urzędzie Miejskim w Zawierciu** organizowano spotkania z mieszkańcami, na których zarówno promowano funkcjonujące formy komunikacji elektronicznej z urzędem, jak również zwracano się do mieszkańców o zgłaszanie propozycji i potrzeb w zakresie rozwijania tej formy komunikacji.*

---

65 Zagadnień dotyczących dostosowania urzędu do elektronicznego świadczenia usług publicznych nie zawarto w dokumentacji strategicznej dwóch miast tj. „Strategii Rozwoju Gminy Zawiercie 2025 plus" i w „Strategii Rozwoju Miasta Mińsk Mazowiecki do roku 2020".

66 UM w: Andrychowie, Głogowie, Legnicy, Lesznie, Mińsk Mazowiecki, Mysłowicach, Płocku, Radomiu, Szczecinku, Śremie i Zawierciu.

67 UM w: Andrychowie, Legnicy, Mińsku Mazowieckim i Zawierciu.

- *W **Urzędzie Miejskim w Andrychowie** przeprowadzono ankietę, w której zawarto pytania odnoszące się do rozpoznania potrzeb mieszkańców w zakresie elektronicznej komunikacji z urzędem: Czy chciałbyś załatwić sprawy w Urzędzie Miejskim w Andrychowie za pośrednictwem usług elektronicznych? Czy byłbyś zainteresowany otrzymaniem bezpłatnego „Profilu Zaufanego"? Wyniki przeprowadzonych badań ankietowych wykazały, że 95% respondentów chciałoby załatwiać sprawy w urzędzie za pośrednictwem usług elektronicznych oraz że 97% ankietowanych byłoby zainteresowanych otrzymaniem bezpłatnego „Profilu Zaufanego" w urzędzie.*

Ponadto, w wyjaśnieniach kontrolowani wskazywali, że przeprowadzano badania ankietowe, na podstawie których uzyskiwano informacje o zadowoleniu mieszkańców z jakości świadczonych usług elektronicznych oraz dane statystyczne o korzystaniu z komunikacji elektronicznej[68]. Dokonywano też analizy poczty elektronicznej[69] wpływającej na skrzynkę ogólną urzędów z uwagami i sugestiami, a także monitorowano środki przekazu (prasa, radio, forum internetowe) celem analizy opinii mieszkańców o funkcjonującej komunikacji elektronicznej z urzędem. Na bieżąco analizowano też statystyki odwiedzin stron internetowych urzędów pod kątem najczęściej wyszukiwanych informacji.

NIK zwraca uwagę na potrzebę podjęcia przez urzędy szerszych działań w zakresie informowania o e-usługach i ich promowania, co mogłoby wpłynąć na większe zainteresowanie mieszkańców możliwością załatwiania spraw w urzędzie drogą elektroniczną. Ma to szczególne znaczenie w sytuacji gdy urzędy świadczą usługi w formie elektronicznej, zaś liczba złożonych dokumentów w tej formie jest znikoma.

W odpowiedziach na wystąpienia pokontrolne kontrolowani informowali o podjętych działaniach w ww. zakresie. Na przykład:

- *Burmistrz **Miasta i Gminy Olkusz** poinformował, że poczynione zostały prace w celu zwiększenia świadomości i upowszechniania wśród obywateli korzyści płynących z korzystania ze środków komunikacji elektronicznej poprzez umieszczenie na stronie internetowej urzędu w zakładce Poradnik Mieszkańca, szczegółowej instrukcji korzystania z platformy ePUAP, jak również informacji o możliwości złożenia wniosku o wydanie profilu zaufanego wraz z wykazem punktów potwierdzających profile zaufane w Olkuszu. Sukcesywnie będą dodawane linki do kolejnych formularzy udostępnianych przez urząd.*
- *Prezydent **Miasta Płocka** podał m.in., że (…) po analizie funkcjonowania obszaru poddanego kontroli podjęto decyzję o zaplanowaniu na przyszły rok akcji informacyjnej dot. funkcjonowania e-administracji (…).*

3.2.3. Obieg dokumentów w urzędach

Zgodnie z § 1 ust. 1 rozporządzenia Prezesa Rady Ministrów z dnia 18 stycznia 2011 r. w sprawie instrukcji kancelaryjnej, jednolitych rzeczowych wykazów akt oraz instrukcji w sprawie organizacji i zakresu działania archiwów zakładowych, określa się m.in. instrukcję kancelaryjną dla organów gminy. W myśl § 1 załącznika nr 1 do ww. rozporządzenia m.in.: czynności kancelaryjne są wykonywane w systemie tradycyjnym lub w systemie Elektronicznego Zarządzania Dokumentacją, tzw. EZD (ust. 2); kierownik podmiotu wskazuje, który z systemów wykonywania czynności kancelaryjnych jest podstawowym sposobem dokumentowania przebiegu załatwiania i rozstrzygania spraw dla danego podmiotu (ust. 3).

We wszystkich objętych badaniem urzędach, w celu zarządzania obiegiem dokumentów i dokumentacją stosowane były procedury i zasady postępowania z dokumentami zawarte w wewnętrznych instrukcjach kancelaryjnych. W 22 z 24 (91,7%) kontrolowanych urzędów jako podstawowy sposób dokumentowania przebiegu załatwiania i rozstrzygania spraw, wskazywano system tradycyjny (papierowy) wykonywania czynności kancelaryjnych w urzędzie.

[68] UM w: Dąbrowie Górniczej, Koszalinie, Lesznie, Mikołowie, Mysłowicach, Olkuszu i Stargardzie Szczecińskim.

[69] UM w Szczecinku.

W dwóch urzędach jako podstawowy sposób dokumentowania przebiegu załatwiania i rozstrzygania spraw, wskazany został system elektronicznego zarządzania dokumentacją. I tak:

- *Proces obiegu dokumentacji oraz zarządzania dokumentami w **Urzędzie Miejskim w Głogowie** regulowała Instrukcja Elektronicznego Obiegu Dokumentów (dalej Instrukcja EOD). Dodatkowo w Regulaminie Organizacyjnym urzędu opisano kwestię opiniowania oraz elektronicznej autoryzacji Zarządzeń Prezydenta włączanych do obiegu elektronicznego, a także wskazano, że sprawy wniesione przez obywateli do urzędu są ewidencjonowane i wprowadzane do elektronicznego systemu EZD. W Instrukcji EOD szczegółowo opisano obieg pism wpływających w formie papierowej oraz elektronicznej, zdefiniowano zadania poszczególnych pracowników urzędu w procesie obiegu dokumentów oraz sprecyzowano jaki rodzaj spraw realizowanych przez poszczególne wydziały oraz komórki organizacyjne nie podlega procedowaniu w obiegu elektronicznym.*
- *Czynności kancelaryjne w **Urzędzie Miejskim w Zawierciu** wykonywane były w systemie EZD, który był podstawowym sposobem dokumentowania przebiegu załatwiania i rozstrzygania spraw w urzędzie od dnia 1 września 2011 r. Procedura elektronicznego obiegu dokumentów w urzędzie regulowała zasady postępowania z dokumentami wpływającymi do urzędu oraz określała czynności od momentu wpływu dokumentów do momentu dostarczenia ich do merytorycznie odpowiedzialnych pracowników. W procedurze nie określono natomiast pozostałych etapów procesu obiegu dokumentów, zawierających m.in. takie elementy jak: akceptacja projektu odpowiedzi na pismo, akceptacja projektu decyzji administracyjnej, postanowienia, itp. oraz wysyłania ich do odbiorcy. W trakcie kontroli NIK dokonano zmiany procedury elektronicznego obiegu dokumentów w urzędzie. Jednak pomimo wprowadzonych zmian wciąż możliwe było wykonywanie niektórych czynności w urzędzie zarówno w formie elektronicznej, jak i papierowej, np. pracownik sporządzający odpowiedź, parafował ją i przekazywał do dalszej akceptacji. Jak podał Sekretarz Miasta Zawiercie, obecnie jest stosowany zarówno papierowy, jak i elektroniczny obieg dokumentów, z przewagą obiegu papierowego. Wyjaśnił też, że urząd jest przygotowany do wprowadzenia systemu elektronicznego jako jedynego funkcjonującego w urzędzie, zarówno pod względem wyposażenia w sprzęt, jak i ludzkim. Jednak dopiero w latach 2017–2018 urząd planuje przejść wyłącznie na elektroniczny obieg dokumentów.*

W 18 urzędach[70] (z 22, tj. w 81,8%) system tradycyjny wykonywania czynności kancelaryjnych wspomagany był przez elektroniczne systemy obiegu dokumentów na różnych etapach załatwiania spraw w urzędzie. Na przykład:

- *W **Urzędzie Miejskim w Chrzanowie** funkcjonował tradycyjny system wykonywania czynności kancelaryjnych z możliwością korzystania z narzędzi informatycznych do wspomagania procesu obiegu dokumentów. Pisma wpływające do urzędu (w tym za pośrednictwem ePUAP) były rejestrowane w systemie informatycznym. W przypadku dokumentów składanych w formie tradycyjnej były one skanowane i wprowadzane do tego systemu, który automatycznie nadawał im kolejny numer w rejestrze. Po zadekretowaniu, za pomocą systemu informatycznego dokumenty przekazywano do wydziałów merytorycznych oraz równolegle do skrzynek poczty elektronicznej kierowników komórek organizacyjnych.*
- *W **Urzędzie Miejskim w Śremie** system tradycyjny wspomagany był przez elektroniczny system obiegu dokumentów, który obsługiwał elektroniczną rejestrację korespondencji, prowadzenie spraw, gromadzenie informacji oraz jej przekazywanie. W wyniku kontroli ustalono, że każdy dokument był skanowany, bądź projekt dokumentu był załączany do danej sprawy w wersji elektronicznej. Jednocześnie w urzędzie stosowano papierową formę dokumentowania przebiegu rozpatrywania spraw.*

Zdaniem NIK, wykorzystywanie systemu tradycyjnego obiegu dokumentów z elementami obiegu elektronicznego powoduje, że te same czynności są częściowo powielane, co niewątpliwie ma wpływ na większe obciążenie pracą urzędników. Istotą wprowadzenia elektronicznego obiegu dokumentów jest usprawnienie i przyśpieszenie obiegu informacji przy jednoczesnej minimalizacji nakładu pracy. Wskazane jest zatem, aby kontynuować działania w celu zapewnienia technicznych i organizacyjnych warunków dla wprowadzenia w urzędach wyłącznie elektronicznego systemu zarządzania dokumentacją, co spowoduje również zmniejszenie zużycia papieru i korzystnie wpłynie na ochronę środowiska.

[70] UM w: Andrychowie, Chrzanowie, Dąbrowie Górniczej, Dzierżoniowie, Koszalinie, Legnicy, Luboniu, Mikołowie, Mińsku Mazowieckim, Mysłowicach, Olkuszu, Ostrowie Wlkp., Płocku, Radomiu, Stargardzie Szczecińskim, Śremie, Świdnicy i Świnoujściu.

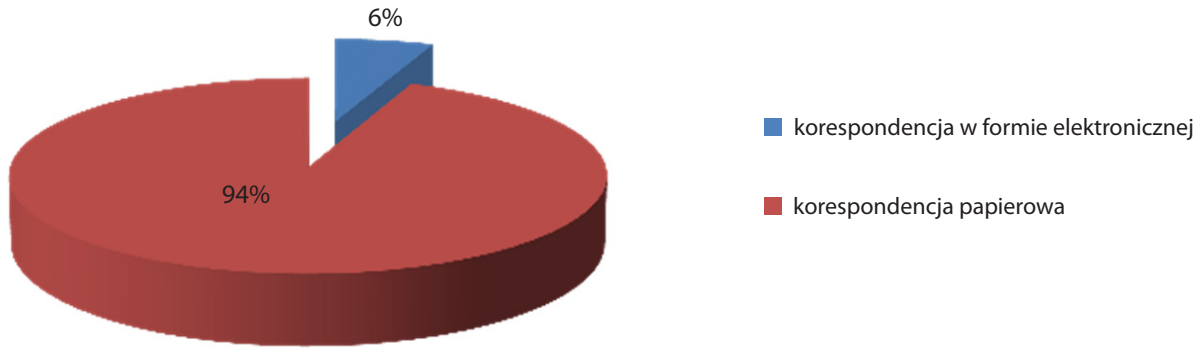
W pozostałych czterech[71] z 22 urzędów (18,2%), nie wprowadzano żadnych elementów elektronicznego obiegu dokumentów i funkcjonował tradycyjny (papierowy) system wykonywania czynności kancelaryjnych. W urzędach tych dokumenty otrzymane drogą elektroniczną były drukowane i dalej rozpatrywane w formie tradycyjnej (papierowej). Na przykład:

- *W **Urzędzie Miejskim w Pruszkowie** nie prowadzono elektronicznego obiegu dokumentów. Dokumenty wpływające do urzędu drogą elektroniczną na konto e-mail prezydent@miasto.pruszkow.pl oraz za pośrednictwem ePUAP były pobierane przez uprawnionych pracowników, drukowane i wpisywane w rejestr papierowy. W przypadku wysyłania dokumentów za pośrednictwem poczty elektronicznej lub ePUAP, dokumenty sporządzone w wersji papierowej były skanowane i wysyłane jako załączniki wiadomości (przy wysyłaniu przez ePUAP przesyłka podpisywana była przez Prezydenta Miasta Pruszkowa profilem zaufanym). Zastępca Prezydenta Miasta Pruszkowa poinformował, że 5 sierpnia 2009 r. Urząd Miejski w Pruszkowie przystąpił do projektu Urzędu Marszałkowskiego Województwa Mazowieckiego pn. Rozwój elektronicznej administracji w samorządach województwa mazowieckiego wspomagającej niwelowanie dwudzielności potencjału województwa, który przewiduje m.in. wdrożenie Elektronicznego Zarządzania Dokumentacją w ramach Systemu e-Urząd. Wdrożenie Elektronicznego Zarządzania Dokumentacją w Urzędzie Miejskim w Pruszkowie przewidziane jest na 1 stycznia 2015 r.*

W sześciu[72] z 18 urzędów (27,3%), w których pomocniczo wykorzystywano system elektronicznego obiegu dokumentów, nie wprowadzono procedur określających zasady ich elektronicznego obiegu w urzędzie. **NIK uważa, że zasadnym jest opracowanie odpowiednich procedur obiegu dokumentów uwzględniających przyjętą praktykę postępowania. Wdrożenie takiej procedury wpłynie zarówno na uporządkowanie i usprawnienie obiegu dokumentów, a także pozwoli wyeliminować równoległe przesyłanie dokumentów papierowych i elektronicznych.**

Z ustaleń kontroli wynika, że w badanym okresie korespondencja skontrolowanych urzędów obejmowała blisko 7 280,4 tys. dokumentów, z tego 3 442,9 tys. stanowiły dokumenty wpływające i 3 837,5 tys. wychodzące. Analiza danych wykazała, że dominującą formą korespondencji była korespondencja tradycyjna (papierowa). Stanowiła ona aż 94% ogółu korespondencji. Korespondencja w formie elektronicznej stanowiła jedynie 6%, z tym, że nieznacznie wyższy udział korespondencji w tej formie wystąpił wśród dokumentów wychodzących niż przychodzących (odpowiednio 6,4% i 5,7%).

Wykres nr 2
Procentowy udział poszczególnych form korespondencji (papierowej i elektronicznej) w korespondencji ogółem prowadzonej w kontrolowanych urzędach w okresie od 31 maja 2012 r do 31 maja 2014 r.



Źródło: Wyniki kontroli.

[71] UM w: Lesznie, Nowym Targu, Pruszkowie, Szczecinku.

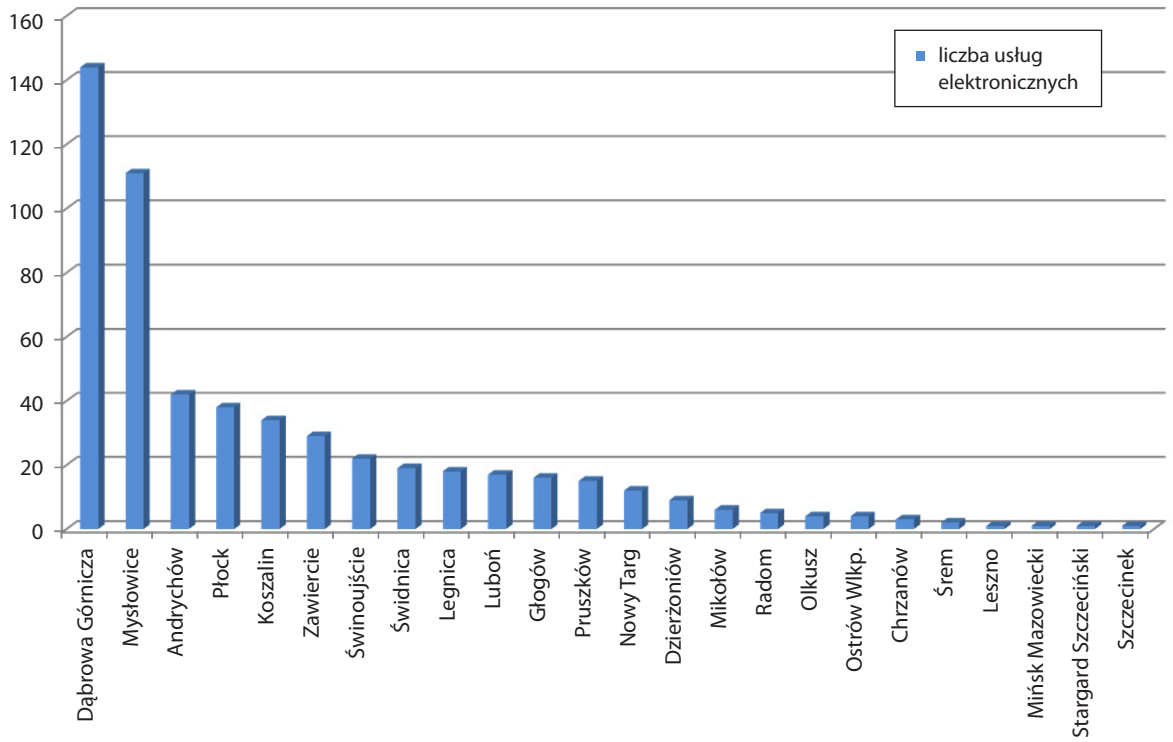
[72] UM w: Legnicy, Luboniu, Mińsku Mazowieckim, Ostrowie Wielkopolskim, Płocku, Świnoujściu.

3.2.4. Usługi elektroniczne

Od usługi w ujęciu tradycyjnym (papierowym) usługę elektroniczną odróżnia świadczenie na odległość oraz ograniczony udział człowieka po stronie urzędu na etapie przyjmowania wniosku. Polega ona na wprowadzeniu przez obywatela wymaganych informacji w formularzu elektronicznym a następnie przesyłanie tych informacji z wykorzystaniem sieci Internet do urzędu. Podstawową usługą elektroniczną świadczoną w jednostkach administracji publicznej jest Elektroniczna Skrzynka Podawcza – miejsce do przyjmowania korespondencji elektronicznej. Obowiązek posiadania ESP przez podmioty publiczne wynika z art. 16 ust. 1a ustawy o informatyzacji.

Kontrola wykazała, że wszystkie objęte badaniem urzędy świadczyły usługi w formie elektronicznej. Liczba tych usług była jednak bardzo zróżnicowana. Ustalono, że w okresie przeprowadzania czynności kontrolnych (czerwiec–wrzesień 2014 r.), w 24 kontrolowanych urzędach udostępniono łącznie 554 e-usług. Do ich udostępniania najczęściej wykorzystywano platformę elektroniczną ePUAP. Korzystano także z platform regionalnych takich jak SEKAP i Cyfrowa Małopolska[73], platform miejscowych, np. Płocka Platforma Teleinformatyczna e-Urząd[74], a także stron internetowych urzędów.

Wykres nr 3
Liczba udostępnionych usług w formie elektronicznej (w okresie przeprowadzania czynności kontrolnych w jednostkach, czerwiec–wrzesień 2014 r.)



Źródło: Wyniki kontroli.

[73] Cyfrowa Małopolska to platforma informatyczna stworzona dla województwa małopolskiego.

[74] Współfinansowaną ze środków UE w ramach Europejskiego Funduszu Rozwoju Regionalnego – Regionalny Program Operacyjny Województwa Mazowieckiego 2007–2013, Priorytet II Przyspieszenie e-rozwoju Mazowsza, Działanie 2.2 Rozwój e-usług. Całkowita wartość projektu – 5.999.859,00 PLN. Wartość dofinansowania – 5.099.880,15 PLN.

Spośród 24 skontrolowanych urzędów, 17[75] (tj. 70,8%) udostępniało mniej niż 20 usług w formie elektronicznej. W pozostałych siedmiu urzędach liczba świadczonych e-usług wynosiła odpowiednio: 22 (UM w Świnoujściu), 29 (UM w Zawierciu), 34 (UM w Koszalinie), 38 (UM w Płocku), 42 (UM w Andrychowie), 111 (UM w Mysłowicach) i 144 (UM w Dąbrowie Górniczej). W grupie urzędów, które udostępniły największą liczbę usług elektronicznych wykorzystano miejską platformę informatyczną. I tak:

- ***Urząd Miasta Płocka,*** *poprzez stronę internetową http://www.plock.eu/pl, udostępnił 31 e-usług świadczonych z wykorzystaniem Płockiej Platformy Teleinformatycznej e-Urząd. Ponadto, za pośrednictwem platformy ePUAP urząd świadczył siedem usług elektronicznych.*
- *W* ***Urzędzie Miejskim w Andrychowie*** *można było skorzystać z czterdziestu dwóch usług elektronicznych, w tym czterech świadczonych poprzez ePUAP, natomiast pozostałe 38 usług było dostępnych z wykorzystaniem portalu Cyfrowa Małopolska.*
- *W* ***Urzędach Miejskich w Dąbrowie Górniczej i w Mysłowicach*** *usługi elektroniczne były udostępniane z wykorzystaniem platformy SEKAP.*

We wszystkich 24 kontrolowanych urzędach udostępniono e-usługę „Pismo ogólne" lub „Skargi, wnioski, zapytania do urzędu", będące formą usługi ESP, która polega na możliwości skierowania pisma do urzędu oraz załączenia do niego odpowiedniego formularza w wersji elektronicznej zapisanego w określonym formacie (np. pdf, .doc).

Ponadto, urzędy świadczyły usługi o charakterze informacyjnym. Usługi te nie były jednak przeznaczone do składania formularzy, wnoszenia podań i wniosków, czyli nie dotyczyły możliwości załatwienia sprawy. Umożliwiły natomiast mieszkańcom elektroniczne zadawanie pytań władzom gminy, wyrażenie opinii na temat projektów aktów prawa miejscowego, sprawdzenie informacji o terminie odbioru dowodu osobistego, wskazanie właściwego obwodu wyborczego czy też zarezerwowanie terminu ślubu w urzędzie stanu cywilnego.

Badanie NIK przeprowadzone w skontrolowanych urzędach na łącznej próbie 114[76] usług elektronicznych (tj. 21,3% ogółu świadczonych usług elektronicznych we wszystkich kontrolowanych urzędach) wykazało, że opisy 98 (tj. 86%) usług zawierały informacje określone w rozporządzeniu ePUAP[77], dotyczące m.in. aktualnej podstawy prawnej świadczonych usług, nazwy usług, miejsca świadczenia usług (złożenia dokumentów), terminu składania i załatwiania spraw oraz nazwy komórek odpowiedzialnych za załatwienie spraw. W przypadku 16 usług[78] objętych badaniem (tj. 14%) stwierdzono, że opisy usług zamieszczone na stronach internetowych urzędów lub na stronach platformy elektronicznej, za pomocą której świadczona była usługa, zawierały nieaktualne lub niekompletne podstawy prawne świadczonych usług. Na przykład:

- *W zamieszonej na stronie BIP* ***Urzędu Miasta Płocka*** *karcie opisu usługi wniosek o wyłączenie gruntów rolnych z produkcji zawarto niewłaściwą podstawę prawną. W karcie tej jako podstawę prawną wskazano ustawę z dnia 3 lutego 1995 r. o ochronie gruntów rolnych i leśnych[79], natomiast zgodnie z art. 5b tej ustawy[80] w brzmieniu obowiązującym w okresie kontroli, przepisów ustawy nie stosowało się do gruntów rolnych stanowiących użytki rolne położonych w granicach administracyjnych miast.*

---

75 UM w (liczba świadczonych e-usług): Lesznie (1), Mińsku Mazowieckim (1), Stargardzie Szczecińskim (1), Szczecinku (1), Śremie (2), Chrzanowie (3), Olkuszu (4), Ostrowie Wlkp. (4), Radomiu (5), Mikołowie (6), Dzierżoniowie (9), Nowym Targu (12), Pruszkowie (15), Głogowie (16), Luboniu (17), Legnicy (18) i Świdnicy (19).

76 Badanie przeprowadzono na losowo wybranej próbie co najmniej pięciu usług świadczonych w formie elektronicznej w 19 skontrolowanych jednostkach. W pozostałych pięciu urzędach, z uwagi na mniejszą liczbę świadczonych e-usług do badania wybrano wszystkie udostępnione usługi elektroniczne.

77 § 8 rozporządzenia ePUAP z 6 maja 2014 r., obowiązującego od 11 maja 2014 r. Poprzednio określone w § 7 ust. 1 rozporządzenia ePUAP z 27 kwietnia 2011 r.

78 Dotyczyło usług świadczonych przez UM w (liczba usług): Lesznie (1), Luboniu (1), Mińsku Mazowieckim (4), Płocku (5) i w Pruszkowie (5).

79 Dz. U. z 2013 r., poz. 1205, ze zm.

80 Przepis wprowadzony na podstawie ustawy z dnia 19 grudnia 2008 r. o zmianie ustawy o ochronie gruntów rolnych i leśnych (Dz. U. Nr 237, poz. 1657). Utracił moc z dniem 5 września 2014 r.

- *Opis pięciu badanych usług elektronicznych świadczonych przez **Urząd Miejski w Pruszkowie** za pośrednictwem ePUAP zawierał nieaktualne wskazania miejsca publikacji (dane promulgacyjne) podstawy prawnej świadczonej usługi. Ponadto, w przypadku jednej usługi pn. Deklaracje o wysokości opłaty za gospodarowanie odpadami komunalnymi, wskazano nieaktualną podstawę prawną, tj. ustawę z dnia 11 maja 2001 r. o opakowaniach i odpadach opakowaniowych[81], która została uchylona pół roku wcześniej, tj. z dniem 1 stycznia 2014 r. NIK zauważa, że w trakcie kontroli w urzędzie podjęto działania mające na celu aktualizację podstawy prawnej w opisach usług. Prezydent Miasta Pruszkowa poinformował, że urząd miejski przygotowuje korektę wszystkich usług na platformie ePUAP.*

Kontrola wykazała, że dwa urzędy[82] na swoich stronach BIP nie zamieściły dla badanych usług elektronicznych informacji odnośnie obowiązujących procedur w zakresie załatwiania spraw drogą elektroniczną. Było to niezgodne z § 5 ust. 2 pkt 4 rozporządzenia KRI, który wskazuje, że interoperacyjność na poziomie organizacyjnym osiągana jest przez publikowanie i uaktualnianie w Biuletynie Informacji Publicznej przez podmiot realizujący zadania publiczne opisów procedur obowiązujących przy załatwianiu spraw z zakresu jego właściwości drogą elektroniczną. Np.:

- ***Urząd Miasta w Mińsku Mazowieckim** na stronie BIP zamieścił link do usługi elektronicznej „skargi, wnioski, zapytania do urzędu". Nie umieścił jednak informacji o procedurze korzystania z tej usługi, co było niezgodne z § 5 ust. 2 pkt 4 rozporządzenia KRI. Burmistrz Miasta Mińsk Mazowiecki podał m.in. że nie widział potrzeby zamieszczenia tej informacji, z uwagi na powszechną znajomość funkcjonowania systemu w zakresie załatwiania spraw drogą elektroniczną przez wszystkich użytkowników Internetu. Stosowna informacja została jednak zamieszczona na stronie BIP urzędu jeszcze w trakcie kontroli NIK.*

Uwagi NIK dotyczyły także niewłaściwego sposobu informowania przez trzy urzędy[83] na własnych stronach internetowych o dostępnych usługach elektronicznych świadczonych za pomocą ePUAP. Na stronach internetowych BIP ww. urzędów zamieszczono tylko ogólny link do platformy ePUAP, a nie do poszczególnych usług tych urzędów, świadczonych za pomocą tej platformy.

Zdaniem NIK, zamieszczenie ogólnego linku do platformy ePUAP jest niewystarczającą informacją o możliwości skorzystania z procedur elektronicznych realizowanych przez urzędy. Umieszczenie bezpośrednich linków do każdej usługi elektronicznej świadczonej za pomocą ePUAP na stronie urzędów oraz na stronie BIP niewątpliwie ułatwiłoby obywatelom dostęp do usług elektronicznych i mogłoby zwiększyć korzystanie z nich.

3.2.5. Centralne repozytorium wzorów dokumentów elektronicznych

Zgodnie z art. 19b ust. 3 ustawy o informatyzacji, organy administracji publicznej przekazują do centralnego repozytorium wzorów dokumentów elektronicznych sporządzone wzory dokumentów elektronicznych.

Spośród 11 urzędów[84], które zobowiązane były do przekazania wzorów dokumentów elektronicznych do CRD, cztery jednostki[85] obowiązek ten zrealizowały. Siedem urzędów[86] nie przekazało wzorów dokumentów elektronicznych do CRD. Było to niezgodne z art. 19b ust. 3 ustawy o informatyzacji. Jako przyczynę wskazywano m.in.: problemy techniczne oraz mylną interpretację ww. przepisu.

81 Dz. U. z 2001 r. Nr 63, poz. 638 ze zm.

82 UM w Mińsku Mazowieckim i w Płocku.

83 UM w: Chrzanowie, Olkuszu i Świnoujściu.

84 UM w: Andrychowie, Dąbrowie Górniczej, Głogowie, Luboniu, Mińsku Mazowieckim, Nowym Targu, Olkuszu, Płocku, Radomiu, Szczecinku i Śremie.

85 UM w: Dąbrowie Górniczej, Mińsku Mazowieckim, Olkuszu i Szczecinku.

86 UM w: Andrychowie, Głogowie, Luboniu, Nowym Targu, Płocku, Radomiu i Śremie.

W większości kontrolowanych urzędów (18[87] spośród 24, tj. 75%) dla wszystkich lub części świadczonych usług elektronicznych wykorzystywano wzory dokumentów elektronicznych pobranych z platformy ePUAP lub platformy SEKAP. W takim przypadku dla urzędu nie występował obowiązek, o którym mowa w art. 19b ust. 3 ustawy o informatyzacji, gdyż skorzystały one z wzorów dokumentów dostępnych w katalogu usług na tych platformach.

Ponadto, w przypadku trzech jednostek[88] wzory dokumentów elektronicznych zostały opracowane przed datą wejścia w życie rozporządzenia Prezesa Rady Ministrów z dnia 14 września 2011 r. w sprawie sporządzania pism w formie dokumentów elektronicznych, doręczania dokumentów elektronicznych oraz udostępniania formularzy, wzorów i kopii dokumentów elektronicznych[89]. W związku z tym dokumenty takie zostały objęte przepisami przejściowymi tego rozporządzenia, które pozwalają na przekazanie wzorów dokumentów do CRD w terminie 5 lat od dnia jego wejścia w życie, tj. nie później niż do 30 października 2016 r. Ustalono, że zgodnie z § 41 ww. rozporządzenia, wzory były opublikowane w lokalnych repozytoriach wzorów dokumentów elektronicznych tych jednostek.

3.2.6. Model usługowy

Zgodnie z § 2 pkt 8 rozporządzenia KRI model usługowy to model, w którym dla użytkowników zdefiniowano stanowiące odrębną całość funkcje systemu teleinformatycznego (usługi sieciowe) oraz opisano sposób korzystania z tych funkcji (inaczej: system zorientowany na usługi).

Zarządzanie usługami elektronicznymi w oparciu o model usługowy jest szczególnie istotne gdy urząd świadczy wiele usług. Sporządzenie kart opisu e-usług pozwala na zawarcie w nich wielu informacji, przez co w momencie wystąpienia awarii urząd jest w stanie szybko powziąć konieczne informacje i przywrócić prawidłowe funkcjonowanie e-usługi. Dokumenty te sporządzane są wyłącznie do użytku wewnątrz urzędu i nie są udostępniane na zewnątrz np. na stronach internetowych.

W badaniu wzięto pod uwagę następujące elementy zarządzania usługami elektronicznymi:

– możliwość zidentyfikowania właściciela (komórki organizacyjnej) poszczególnych usług świadczonych przez urząd,
– ustalenie sposobu zgłaszania awarii, osoby/komórki/podmiotu odpowiedzialnego za usuwanie awarii, technicznego właściciela usługi,
– określenie maksymalnego czasu niedostępności e-usługi.

Ustalenia kontroli wskazują, że wszystkie kontrolowane jednostki w podstawowym zakresie wspierały model usługowy w procesie świadczenia usług elektronicznych. Badanie przeprowadzone na łącznej próbie 114 usług świadczonych w formie elektronicznej wykazało, że dokumentacja opisująca e-usługi umożliwiała zidentyfikowanie właścicieli świadczonych usług, tj. komórek organizacyjnych odpowiedzialnych za realizację usług. Ze względu na fakt, że usługi świadczone były za pośrednictwem niezależnych od urzędów platform (m.in. ePUAP, którą zarządza Centrum Projektów Informatycznych MAiC i SEKAP, której administratorem jest Śląskie Centrum Społeczeństwa Informacyjnego), urzędy nie miały możliwości technicznej ingerencji w ich funkcjonowanie. Tym samym nie wskazywano maksymalnego ani dopuszczalnego czasu niedostępności e-usług, sposobu zgłaszania awarii oraz osób/komórek/podmiotów odpowiedzialnych za usuwanie awarii.

87 UM w: Andrychowie, Chrzanowie, Dąbrowie Górniczej, Dzierżoniowie, Koszalinie, Legnicy, Lesznie, Luboniu, Mikołowie, Mysłowicach, Olkuszu, Ostrowie Wlkp., Pruszkowie, Radomiu, Stargardzie Szczecińskim, Śremie, Świdnicy i Świnoujściu.

88 UM w: Koszalinie, Płocku i Zawierciu.

89 Dz. U. Nr 206 poz. 1216 ze zm.

3.2.7. Współpraca wybranych systemów informatycznych z innymi systemami

Dla potrzeb oceny stopnia współpracy systemów informatycznych z innymi systemami urzędu przyjęto na podstawie opracowania Ministra Administracji i Cyfryzacji *Polska 2030 Przyszłość polskich regionów w perspektywie rozwoju społeczeństwa cyfrowego*[90] następującą klasyfikację poziomów współpracy:

1) transakcyjny czyli wymiana danych pomiędzy systemami bez jakiegokolwiek pośrednictwa pracownika, czyli przekazywanie danych odbywa się w sposób w pełni zautomatyzowany,
2) dwustronnej komunikacji, tj. dane z systemu A przekazywane są do systemu B, przy czym system B samodzielnie odnotowuje, że oczekują dane, które mogą być zaimportowane. Rolą pracownika jest udzielenie zgody (zatwierdzenie) w systemie B na wczytanie otrzymanych danych. Odpowiedź z systemu B do systemu A jest przekazywana analogicznie,
3) jednostronnej komunikacji, tj. dane z jednego systemu są przekazywane do innego systemu za pośrednictwem pracownika (operatora systemu), który ręcznie dane te importuje,
4) informacyjny – gdy pracownicy wiedzą że konkretne systemy gromadzą dane i że w razie potrzeb mogą z nich skorzystać, znają też sposób dostępu do danych zgromadzonych w systemach, np. jak wygenerować odpowiednie dane do pliku.

Brak współpracy (interoperacyjności) wystąpi wówczas, gdy system nie komunikuje się z żadnym innym systemem informatycznym, jest samodzielny, wszystkie bazy danych są zasilane ręcznie przez wprowadzanie danych. Nie ma możliwości wygenerowania danych do pliku (możliwe jest jedynie odczytanie informacji z takiego systemu).

Do badania zakresu i sposobu współpracy systemów informatycznych wewnątrz urzędów wybrano w sposób celowy[91] 79 systemów informatycznych zakupionych lub zmodernizowanych po 31 maja 2012 r. (tj. po wejściu w życie rozporządzenia KRI). Ocenie w zakresie współpracy systemów informatycznych wewnątrz urzędów poddano 77 z 79 objętych kontrolą systemów informatycznych, gdyż dwa systemy ze względu na swoją specyfikę nie wymagały komunikowania się z innymi systemami gdyż były to narzędzia wspomagające pracę na pojedynczych stanowiskach pracy. Spośród 77 ocenianych systemów informatycznych 72 systemy, tj. 93,5% współpracowały z innymi systemami informatycznymi kontrolowanych urzędów i tym samym spełniały minimalne wymogi interoperacyjności, o których mowa w § 5 ust. 3 pkt 3 rozporządzenia KRI, a pięć[92] systemów (tj. 6,5%) nie spełniało minimalnych wymogów interoperacyjności. W szczególności:

- Dwanaście[93] z 72 systemów (16,7%) zapewniało współpracę na poziomie najbardziej dojrzałym, tj. transakcyjnym, co oznacza, że przekazywanie danych odbywało się w sposób w pełni zautomatyzowany. Na przykład:
  - *W **Urzędzie Miejskim w Pruszkowie** badany system do rejestracji wpłat z tytułu opłat za gospodarowanie odpadami komunalnymi (dalej GOK) wymieniał bezpośrednio dane z systemem podatków i opłat oraz z systemem opłat lokalnych. System GOK automatycznie przesyłał dane (np. o wysokości zaksięgowanej wpłaty z tytułu opłaty za gospodarowanie odpadami komunalnymi) do ww. dwóch systemów oraz automatycznie pobierał dane z tych systemów dotyczące (np. wysokości naliczonej opłaty za gospodarowanie odpadami komunalnymi).*

90 Warszawa, 6 czerwca 2012 r., str. 9, www.mir.gov.pl/aktualnosci/polityka_rozwoju/Documents/Prezentacja_MinBoni.pdf

91 Przy wyborze systemów do badania kierowano się ich funkcjonalnością wykorzystywaną do obsługi interesantów.

92 Wykorzystywanych w trzech UM w (liczba systemów informatycznych): Dąbrowie Górniczej (1), Szczecinku (1) i Zawierciu (3).

93 Systemy wykorzystywane w siedmiu UM w (liczba systemów informatycznych): Dzierżoniowie (3), Głogowie (1), Legnicy (2), Lesznie (1), Mikołowie (1), Pruszkowie (3) i Świdnicy (1).

- *W **Urzędzie Miasta Legnicy** program służący do obsługi deklaracji i należności z tytułu gospodarki odpadami komunalnymi pobierał automatycznie dane osobowe i adresowe oraz dane o powierzchni opodatkowanej z innych programów. Generował dokumenty księgowe i przekazywał dane dotyczące należności i zobowiązań do oprogramowania księgowego.*
- *W **Urzędzie Miasta Dzierżoniów** badany system służący do elektronicznego zarządzania dokumentacją w ramach którego prowadzony był Centralny Rejestr Umów wymieniał dane dotyczące identyfikatora sprawy, daty i godziny ostatniej modyfikacji sprawy, numeru i przedmiotu umowy oraz wartości zamówienia a także statusu i nazwy instytucji. Wymiana danych następowała z systemem odpowiedzialnym za ich publikację w BIP.*

- Siedemnaście systemów (23,6%) zapewniało współpracę na poziomie dwustronnej komunikacji. Wymiana danych pomiędzy systemami następowała po wcześniejszym zatwierdzeniu przez pracownika danych wysyłanych z systemu, jak i danych importowanych z innych systemów. Na przykład:
  - *W **Urzędzie Miejskim w Świdnicy** system gospodarowania odpadami komunalnymi, służący do gromadzenia informacji niezbędnych do prawidłowego funkcjonowania w urzędzie ewidencji związanej z gospodarowaniem odpadami komunalnymi pobierał dane osobowe z systemu ewidencji ludności oraz dane ewidencyjne z systemu naliczania podatków od gruntów i nieruchomości. W przypadku nowego obiektu, wprowadzone do systemu gospodarowania odpadami dane mogły być wysłane do współpracujących ww. systemów.*
  - *W **Urzędzie Miejskim w Śremie** system wykorzystywany do prowadzenia ewidencji oraz naliczania opłat w zakresie wycinki drzew czy z tytułu posiadania psa wymieniał dane osobowe mieszkańców i adresów nieruchomości z systemem służącym do rejestracji i modyfikacji danych umieszczonych w kartach osobowych mieszkańców.*
  - *W **Urzędzie Miasta Świnoujście** system elektronicznego obiegu dokumentów współpracował z systemem ePUAP – pobierał i wysyłał dokumenty wytworzone w formie elektronicznej.*
- Pozostałe 43 (59,7%) systemy informatyczne zapewniały poziom jednostronnej komunikacji, bądź poziom informacyjny. W przypadku jednostronnej komunikacji, wymiana danych polegała m.in. na tym, że pracownik tworzył zbiór niezbędnych danych i importował do własnego systemu informatycznego lub eksportował do innego. Poziom informacyjny systemów informatycznych urzędów zapewniony był wówczas, gdy pracownik posiadał wiedzę o możliwości skorzystania z danych zawartych w innych systemach i mógł je wykorzystać. Na przykład:
  - *W **Urzędzie Miasta w Szczecinku** system służący do ewidencjonowania deklaracji o wysokości opłat za gospodarowanie odpadami komunalnymi zapewniał poziom jednostronnej komunikacji. Pracownik przesyłał dane do systemu finansowo – księgowego. Natomiast system dotyczący rozliczania tytułów wykonawczych jednostronnie komunikował się z systemem finansowo-księgowym w ten sposób, że pracownik importował do systemu rozliczania tytułów wykonawczych dane w zakresie tytułu wykonawczego.*
  - *W **Urzędzie Miejskim w Chrzanowie** system informatyczny obsługi urzędu stanu cywilnego zapewniał poziom informacyjny. Podczas rejestracji aktu urodzenia/małżeństwa/zgonu, po wprowadzeniu nr PESEL można było pobrać niezbędne dane z systemu ewidencji ludności (imiona, nazwisko, nazwisko rodowe, datę i miejsce urodzenia, stan cywilny, adres zameldowania, numer dokumentu tożsamości).*

Ponadto, kontrola wykazała, że jedynie pięć[94] spośród 72, tj. 6,9% badanych systemów informatycznych, odwoływało się bezpośrednio do danych gromadzonych w innych systemach/rejestrach publicznych (zasada referencji). Trzy systemy informatyczne wspomagające obsługę ewidencji ludności w urzędzie[95] wykorzystywały odwołania do rejestru centralnego PESEL. W przypadku dwóch systemów wykorzystywanych w UM w Pruszkowie pobierały one on-line dane z Systemu Informacji Przestrzennej Starostwa Powiatowego w Pruszkowie dotyczące granic działek i budynków komunalnych oraz obszarów chronionych. Pozostałe badane systemy IT korzystały wyłącznie z własnych zbiorów danych urzędów.

[94] Wykorzystywanych w czterech UM w (liczba systemów IT): Chrzanowie (1), Głogowie (1), Pruszkowie (2) i Radomiu (1).

[95] Dotyczy UM w: Chrzanowie, Głogowie i Radomiu.

3.3 Wdrożenie systemu zarządzania bezpieczeństwem systemów informatycznych

Przepis § 20 ust. 1 rozporządzenia KRI stanowi m.in., że podmiot realizujący zadania publiczne opracowuje i ustanawia, wdraża i eksploatuje, monitoruje i przegląda oraz utrzymuje i doskonali system zarządzania bezpieczeństwem informacji zapewniający poufność, dostępność i integralność informacji. Zgodnie z § 20 ust. 2 pkt 1 ww. rozporządzenia, podmiot ten zobowiązany jest do zapewnienia aktualizacji regulacji wewnętrznych w zakresie dotyczącym zmieniającego się otoczenia.

Zgodnie z § 20 ust. 3 rozporządzenia KRI, obowiązki, o których mowa w § 20 ust. 1 i 2 rozporządzenia KRI uznaje się za spełnione, jeżeli system zarządzania bezpieczeństwem informacji został opracowany na podstawie Polskiej Normy PN-ISO/IEC 27001, a ustanawianie zabezpieczeń, zarządzanie ryzykiem oraz audytowanie odbywa się na podstawie Polskich Norm związanych z tą normą, w tym: PN-ISO/IEC 17799 – w odniesieniu do ustanawiania zabezpieczeń; PN-ISO/IEC 27005 – w odniesieniu do zarzadzania ryzykiem; PN-ISO/IEC 24762 – w odniesieniu do odtwarzania techniki informatycznej po katastrofie w ramach zarządzania ciągłością działania.

3.3.1. Dokumenty z zakresu bezpieczeństwa informacji

Ustalenia kontroli wskazują, że w 15[96] objętych kontrolą urzędach, tj. 62,5%, nie opracowano i nie wdrożono całościowej Polityki Bezpieczeństwa Informacji, która jest istotnym elementem systemu zarządzania bezpieczeństwem informacji. Przepis § 20 ust. 1 rozporządzenia KRI zobowiązuje podmioty realizujące zadania publiczne m.in. do opracowania, ustanowienia, wdrożenia, monitorowania i dokonywania przeglądów systemu zarządzania bezpieczeństwem informacji. W myśl § 20 ust. 3 tego rozporządzenia wymagania w zakresie systemu zarządzania bezpieczeństwem informacji uznaje się za spełnione, jeżeli system ten został opracowany na podstawie Polskich Norm[97]. W pkt 5.1 normy PN-ISO/IEC 17799:2007 wskazano opracowanie i stosowanie dokumentu polityki bezpieczeństwa informacji.

Opracowane i wdrożone w tych jednostkach regulacje dotyczące zagadnień związanych z zarządzaniem bezpieczeństwem informacji **nie obejmowały wszystkich informacji jakie są przetwarzane w urzędzie[98], lecz dotyczyły głównie danych osobowych.** W wyjaśnieniach wskazywano m.in., że planowane są, bądź podjęto już prace dla przygotowania nowej Polityki Bezpieczeństwa Informacji, która obejmie wszystkie elementy systemu zarządzania bezpieczeństwem informacji w urzędzie. Na przykład:

- *W **Urzędzie Miasta i Gminy Olkusz** w 2004 r. opracowano Politykę bezpieczeństwa dla przetwarzania danych osobowych. Nie dotyczyła ona jednak wszystkich danych jakie są przetwarzane w urzędzie. Nie uwzględniała np. zmian wprowadzonych w 2012 r., zasad obiegu korespondencji w związku z wprowadzeniem systemu obiegu dokumentów elektronicznych, systemów zakupionych lub zmodernizowanych po 31 maja 2012 r. W odpowiedzi na wystąpienie pokontrolne Burmistrz wskazał, że wdrożenie Polityki Bezpieczeństwa Informacji określającej zasady bezpieczeństwa informacji nastąpi w pierwszym kwartale 2015 r.*

[96] Dotyczy UM w: Andrychowie, Dąbrowie Górniczej, Dzierżoniowie, Głogowie, Lesznie, Luboniu, Mikołowie, Mińsku Mazowieckim, Olkuszu, Ostrowie Wlkp., Pruszkowie, Radomiu, Stargardzie Szczecińskim, Świnoujściu i Zawierciu.

[97] Polska Norma PN-ISO/IEC 27001:2007 *Technika informatyczna. Techniki bezpieczeństwa. Systemy zarządzania bezpieczeństwem informacji. Wymagania* oraz powiązana z nią Polska Norma PN-ISO/IEC 17799:2007 *Technika informatyczna. Techniki bezpieczeństwa. Praktyczne zasady zarządzania bezpieczeństwem informacji.*

[98] M.in. dotyczących konfiguracji infrastruktury informatycznej w tym serwerów, zarządzania hasłami dostępu do systemów IT, treści umów z dostawcami, warunków zastrzeżonych przez dostawców, tajemnic wynikających z innych aktów prawnych, jak np. prawa własności intelektualnej, zasad bezpieczeństwa fizycznego w obiekcie, korespondencji służbowej czy stosowanych zabezpieczeń systemów informatycznych.

- *W **Urzędzie Miejskim w Dąbrowie Górniczej** w czerwcu 2013 r. wprowadzono Politykę Bezpieczeństwa danych osobowych przetwarzanych w Urzędzie Miasta, do której załącznikiem była Instrukcja zarzadzania systemami informatycznymi służącymi do przetwarzania danych osobowych. Dokumenty te nie obejmowały wszystkich informacji jakie są przetwarzane w urzędzie lecz odnosiły się głównie do danych osobowych. Pełnomocnik ds. Informacji Niejawnych wyjaśnił m.in., że opracowywany jest nowy dokument – Polityka Bezpieczeństwa Informacji, który będzie określał nie tylko zakres ochrony danych osobowych, ale wszelkie ważne informacje dla jednostki oraz zasady i szczegóły zabezpieczeń stosowanych w urzędzie, a w tym sposób przepływu danych pomiędzy poszczególnymi systemami, opis struktury zbiorów danych, procedury rozpoczęcia, zawieszenia i zakończenia pracy, przeznaczone dla użytkowników systemu. Nowa Polityka Bezpieczeństwa Informacji zostanie wprowadzona w 2015 r.*
- *W **Urzędzie Miejskim w Stargardzie Szczecińskim** obowiązująca w urzędzie dokumentacja PBI obejmowała zagadnienia dotyczące m.in. wyznaczania administratora bezpieczeństwa, sposobu zarządzania danymi osobowymi, postępowania w sytuacji naruszenia ochrony danych osobowych. Jak wyjaśnił Prezydent Miasta, po wejściu w życie rozporządzenia KRI (…) został rozszerzony obowiązek utworzenia zestawów procedur bezpieczeństwa i zasad wraz z ich udokumentowaniem, planem wdrożenia i egzekwowaniem. Dotychczasowa PBI (…) wymagała szczegółowego rozszerzenia poszczególnych zapisów (np. polityka haseł, bezpieczeństwa systemów, kopii awaryjnych, procedur rozpoczęcia i zakończenia pracy, konserwacji, przechowywania i zabezpieczenia danych (…). W związku z tym został rozpoczęty proces aktualizacji dokumentacji (…). W odpowiedzi na wystąpienie pokontrolne Prezydent Miasta poinformował, iż zaktualizowana Polityka Bezpieczeństwa Informacji[99] została już opracowana i wdrożona.*

Pozostałe dziewięć urzędów[100] objętych badaniem (tj. 37,5%), opracowało i wdrożyło procedury regulujące politykę bezpieczeństwa informacji, jednak w przypadku dwóch z tych jednostek[101] w okresie objętym kontrolą nie dokonywano aktualizacji przyjętych procedur, co było niezgodne z § 20 ust. 2 pkt 1 ww. rozporządzenia, który stanowi, że podmiot realizujący zadania publiczne zobowiązany jest do zapewnienia aktualizacji regulacji wewnętrznych w zakresie dotyczących zmieniającego się otoczenia. Należy zauważyć, że na potrzebę zaktualizowania obowiązujących w tych urzędach polityk bezpieczeństwa wskazywały zalecenia z przeprowadzonych w 2013 r. audytów wewnętrznych z zakresu bezpieczeństwa informacji.

3.3.2. Dokonywanie analizy zagrożeń związanych z przetwarzaniem informacji

Zgodnie z § 20 ust. 2 pkt 3 rozporządzenia KRI należy realizować działania dotyczące przeprowadzania okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji oraz podejmować działania minimalizujące to ryzyko, stosownie do przeprowadzonej analizy.

Kontrola wykazała, że w zdecydowanej większości jednostek (22, tj. w 91,7%) w okresie objętym kontrolą przeprowadzano okresowe analizy utraty integralności, poufności lub dostępności informacji. W analizach zidentyfikowano m.in. ryzyka braku ciągłości pracy jednostki, a także dla każdego ryzyka określano planowane działania mające na celu jego ograniczenie oraz koszty tych działań. Na przykład:

- *W **Urzędzie Miejskim w Pruszkowie**, stosownie do wyników przeprowadzonej analizy, podjęto działania w celu wyeliminowania stwierdzonych ryzyk, w tym założono instalację przeciwpożarową w całym budynku, przeniesiono zasilacze awaryjne (UPS-y) do nowej lokalizacji i zainstalowano dodatkową klimatyzację, rozbudowano serwerownię, wygospodarowano dodatkowe fundusze na wymianę sprzętu komputerowego z bezpieczniejszym systemem operacyjnym w związku z zaprzestaniem przez firmę Microsoft aktualizacji dotychczas zainstalowanego systemu Windows XP i oprogramowania serwerowego Windows 2003.*

[99] Zarządzenie nr 255/2014 Prezydenta Miasta Stargardu Szczecińskiego z dnia 30 października 2014 r. w sprawie organizacji zarządzania bezpieczeństwem przetwarzanych informacji w Urzędzie Miejskim w Stargardzie Szczecińskim.

[100] UM w: Chrzanowie, Koszalinie, Legnicy, Mysłowicach, Nowym Targu, Płocku, Szczecinku, Śremie i Świdnicy.

[101] Dotyczy UM w: Koszalinie i Nowym Targu.

W dwóch urzędach[102] w okresie objętym kontrolą nie przeprowadzano okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji, co było niezgodne z § 20 ust. 2 pkt 3 rozporządzenia KRI. Jak wskazali kontrolowani, analizy takie przeprowadzone zostaną do końca 2014 r. **Zdaniem NIK, szybki postęp technologiczny w środowisku informatycznym i pojawianie się nowych ryzyk dla bezpieczeństwa informacji wskazuje na potrzebę przeprowadzenia analiz ryzyka utraty integralności, dostępności lub poufności informacji, zwłaszcza, że od wejścia w życie rozrządzenia KRI do dnia zakończenia kontroli upłynęło ponad dwa lata.** Wskazanym jest przy tym, aby analizy takie poprzedzały przeprowadzenie obowiązkowego corocznego audytu wewnętrznego w zakresie bezpieczeństwa informacji, o którym mowa w § 20 ust. 2 pkt 14 rozporządzenia KRI. Pozwoliłoby to bowiem na objęcie audytem tych zagadnień, w których ujawniono najwyższe ryzyka wystąpienia zagrożeń.

3.3.3. Inwentaryzacja sprzętu informatycznego

Zgodnie z § 20 ust. 2 pkt 2 rozporządzenia KRI zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez utrzymywanie aktualności inwentaryzacji sprzętu i oprogramowania służącego do przetwarzania informacji obejmującej ich rodzaj i konfigurację. Ponadto, zgodnie z pkt 7.1.1 normy PN-ISO/IEC 17799:2007, wszystkie aktywa informatyczne powinny być zidentyfikowane oraz powinien być sporządzany i aktualizowany ich spis. Aktualna inwentaryzacja sprzętu informatycznego i oprogramowania powinna także zawierać informację o jego rodzaju i konfiguracji, przez co możliwe będzie odtworzenie po katastrofie lub innym zdarzeniu losowym.

Ustalono, że w czterech urzędach[103] (z 23[104], tj. 17,4%) nie prowadzono inwentaryzacji zasobów informatycznych, w sposób określony w § 20 ust. 2 pkt 2 rozporządzenia KRI. Dane sprzętu komputerowego ujmowano w układzie kart informacyjnych lub tradycyjnej książki inwentarzowej dla potrzeb rachunkowości. Nie zawierały one jednak szczegółowych danych o konfiguracji technicznej urządzeń czy też o zainstalowanym na nich oprogramowaniu. Na przykład:

- *W **Urzędzie Miejskim w Pruszkowie**, jak wyjaśnił Prezydent Miasta Pruszkowa, prowadzona jest inwentaryzacja zasobów elektronicznych w wersji papierowej. Na kartach wpisane są podstawowe parametry stanowiska komputerowego (licencje systemowe, oprogramowanie biurowe) wraz z informacjami do jakiego typu aplikacji jest komputer przeznaczony. NIK ustaliła, że prowadzona inwentaryzacja zasobów elektronicznych w wersji papierowej obejmowała zaledwie 16% używanego w urzędzie sprzętu informatycznego oraz nie zawierała istotnych informacji o rodzaju i konfiguracji urządzeń.*

Ponadto, kontrola NIK wykazała, że w dwóch urzędach (tj. 8,7%) inwentaryzacja prowadzona była w sposób nierzetelny. I tak:

- *W **Urzędzie Miejskim w Głogowie** w programie inwentaryzacyjnym brak było informacji o ośmiu komputerach i dwóch serwerach. Natomiast w Urzędzie Miasta w Mińsku Mazowieckim na 10 zbadanych komputerów, w trzech przypadkach wystąpiły różnice między faktycznie zainstalowanymi na tych komputerach programami, a wykazanymi w aplikacji inwentaryzacyjnej.*

Zdaniem NIK, prowadzenie inwentaryzacji zawierającej dane szczegółowe o konfiguracji technicznej urządzeń oraz o zainstalowanym na nich oprogramowaniu może ułatwić sprawne odtworzenie zasobów informatycznych w razie wystąpienia zdarzeń losowych jak np. kradzież lub poważna awaria sprzętu informatycznego.

[102] UM: Leszno i Nowy Targ.

[103] Dotyczy UM w: Nowym Targu, Olkuszu, Pruszkowie i Świnoujściu.

[104] Badania nie przeprowadzono w Urzędzie Miasta Płocka ze względu na trwającą w trakcie kontroli migrację danych do nowo zakupionego programu inwentaryzacyjnego.

3.3.4. Zarządzanie uprawnieniami do pracy w systemach informatycznych

W myśl § 20 ust. 2 pkt 4 i 5 rozporządzenia KRI, zarządzanie bezpieczeństwem informacji realizowane jest m.in. przez podejmowanie działań zapewniających, że osoby zaangażowane w proces przetwarzania informacji posiadają stosowne uprawnienia i uczestniczą w tym procesie w stopniu adekwatnym do realizowanych przez nie zadań oraz obowiązków, a w przypadku zmiany zadań następuje również zmiana uprawnień.

Ustalono, że z wyjątkiem jednego urzędu[105] wszystkie kontrolowane urzędy opracowały i wdrożyły pisemne procedury zarządzania uprawnieniami użytkowników w systemach informatycznych. Jednak w ośmiu[106] (tj. 33,3%) skontrolowanych urzędach stwierdzono nieprawidłowości polegające na niedochowaniu niektórych wymogów określonych w ww. przepisach rozporządzenia KRI i nie przestrzeganiu w tych urzędach wewnętrznych procedur zarządzania uprawnieniami do pracy w systemach informatycznych.

W wyniku badania przyznanych uprawnień dostępu do korzystania z systemów informatycznych, dokonanego na łącznej próbie 421 pracowników kontrolowanych urzędów stwierdzono, że w przypadku 18 osób[107] (4,3%) wystąpiły nieprawidłowości w zakresie nadawania uprawnień do realizowanych zadań. W przypadku 11 z tych osób[108] nadane uprawnienia były nieadekwatne do zadań określonych w zakresach czynności tych osób, co było niezgodne z § 20 ust. 2 pkt 4 rozporządzenia KRI. W wyjaśnieniach wskazywano, że nadane uprawnienia wynikały z racji faktycznie wykonywanych przez te osoby obowiązków, bądź że osoby posiadały dostęp do programu z uwagi na konieczność obsługi klientów podczas nieobecności upoważnionych pracowników. W przypadku pozostałych siedmiu osób nieprawidłowości dotyczyły:

– nadania przez Administratora Systemu Informatycznego uprawnień dwóm pracownikom, pomimo, że nie posiadali oni upoważnienia burmistrza, przyznania uprawnienia kolejnym dwóm niezgodnie z upoważnieniami, oraz nieprzyznania jednemu pracownikowi uprawnień do pracy w systemie, pomimo posiadanego przez niego upoważnienia burmistrza[109],
– braku upoważnienia do obsługiwanego systemu informatycznego dla dwóch pracowników[110].

W wyniku badania blokowania lub odbierania dostępu do systemów informatycznych na próbie 310 pracowników, którzy zakończyli zatrudnienie w okresie objętym kontrolą, stwierdzono, iż dwudziestu byłym pracownikom (tj. 6,5%) siedmiu urzędów[111] konta nie zostały zablokowane i pozostawały wciąż aktywne. Zakres nieodebranych uprawnień, jak i okres po jakim zablokowano dostęp do kont był w poszczególnych urzędach zróżnicowany, np.:

- *W **Urzędzie Miasta Płocka** konta 10 z 24 byłych pracowników nie zostały zablokowane, a działania dla zablokowania kont podjęto dopiero w trakcie kontroli NIK.*
- *W **Urzędzie Miasta Świnoujście** czterem z 10 pracowników zablokowano konta po upływie od trzech do ośmiu miesięcy od dnia zakończenia zatrudnienia.*
- *W **Urzędzie Miejskim w Pruszkowie** dwóm 10 pracowników zablokowano konta użytkowników dopiero w trakcie kontroli, po upływie ponad pół roku od zakończenia przez nich pracy w urzędzie.*

105 UM w Stargardzie Szczecińskim.
106 UM w: Dzierżoniowie, Głogowie, Lesznie, Mikołowie, Mińsku Mazowieckim, Płocku, Pruszkowie i Świnoujściu.
107 Dotyczy UM w: Mikołowie (dwie osoby), Mińsku Mazowieckim (pięć osób), Płocku (trzy osoby), Świnoujściu (osiem osób).
108 Urząd Miasta Świnoujście (osiem osób), Urząd Miasta Płocka (trzy osoby).
109 UM w Mińsku Mazowieckim.
110 UM Mikołów.
111 UM w (liczba osób): Dzierżoniowie (1), Głogowie (1), Lesznie (1), Mińsku Mazowieckim (1), Płocku (10), Pruszkowie (2), Świnoujściu (4).

NIK zwróciła uwagę na konieczność podejmowania działań zapewniających, iż osoby zaangażowane w proces przetwarzania informacji posiadają stosowne uprawnienia i uczestniczą w tym procesie w stopniu adekwatnym do realizowanych przez nie zadań oraz obowiązków. Zwróciła również uwagę na konieczność dokonywania bezzwłocznej zmiany uprawnień, bądź blokowania lub odbierania uprawnień, w przypadku zmiany zadań lub ustania zatrudnienia.

Ponadto, w trakcie kontroli ustalono, że spośród 350 objętych badaniem pracowników, wykonujących zadania w systemach informatycznych 82 z nich, tj. 23,4%, miało możliwość zainstalowania na użytkowanych komputerach dowolnego oprogramowania. Sytuacja taka wystąpiła w dziewięciu urzędach[112] i dotyczyła od 6,7% do 100% objętych badaniem pracowników w poszczególnych urzędach. W czterech urzędach[113] wszyscy badani użytkownicy systemów informatycznych niebędący pracownikami służb informatycznych posiadali uprawnienia administratora systemu na używanych przez nich komputerach, w związku z czym mogli samodzielnie instalować dowolne oprogramowanie. Powyższe nieprawidłowości tłumaczono m.in. następująco:

- *Burmistrz **Miasta Szczecinek** wyjaśnił: Cztery komputery, spośród badanych dziesięciu komputerów, które podlegały badaniu przeprowadzonym 9 lipca 2014 r., przypisane są pracownikom wyższej kadry zarządzającej o najwyższej świadomości użytkowników. Na tych stanowiskach wymagana jest odpowiedzialność również w dziedzinie korzystania ze sprzętu technologii informatycznej.*
- *Burmistrz **Miasta Lubonia** wyjaśnił m.in., że przyjęte rozwiązanie wynikało z braków kadrowych (w urzędzie zatrudniony był jeden informatyk oraz jedna osoba na stanowisku pomocy administracyjnej posiadająca wiedzę informatyczną), zaś każdy z pracowników podpisał oświadczenie o niepodejmowaniu prób instalacji oprogramowania innego niż pochodzącego od pracodawcy.*

Zdaniem NIK, potrzeba ograniczania uprawnień pracowników urzędów wynika także z konieczności ograniczenia ryzyka nieświadomego zainstalowania przez użytkownika złośliwego oprogramowania w trakcie przeglądania stron internetowych. Oprogramowanie antywirusowe i inne wewnętrzne systemy zabezpieczające bez tego ograniczenia nie dają wystarczającej gwarancji bezpiecznej pracy w systemie informatycznym.

Ponadto, w jednym urzędzie[114] stwierdzono, że w 14 przypadkach logowanie do komputerów następowało bez podania hasła. Burmistrz Miasta wyjaśnił m.in., że nie zostały one zabezpieczone hasłem dla wygody pracy pracowników zastępujących danego pracownika. Zadeklarował, że wszystkie komputery zostaną zabezpieczone do końca września 2014 r. NIK zwróciła uwagę, że zgodnie z § 20 ust. 2 pkt 7 rozporządzenia KRI przetwarzane informacje powinny być chronione przed ich kradzieżą i nieuprawnionym dostępem. Podstawową zaporą ochronną przed dostępem osób nieuprawnionych jest zabezpieczenie komputera służbowego hasłem użytkownika.

3.3.5. Szkolenia pracowników zaangażowanych w proces przetwarzania informacji

Zgodnie z § 20 ust. 2 pkt 6 rozporządzenia KRI zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez zapewnienie przez kierownictwo podmiotu publicznego warunków umożliwiających realizację i egzekwowanie szkolenia osób zaangażowanych w procesie przetwarzania informacji.

W 17 urzędach[115], tj. w 70,8% kontrolowanych urzędów zorganizowano szkolenia dotyczące bezpieczeństwa informacji dla pracowników urzędów. Tematyka szkoleń dotyczyła m.in. postępowania z informacją w urzędzie (w tym ochrony danych osobowych informacji niejawnych), bezpieczeństwa

[112] UM w: Chrzanowie, Głogowie, Luboniu, Mińsku Mazowieckim, Nowym Targu, Olkuszu, Pruszkowie, Szczecinku i Świnoujściu.

[113] UM w: Luboniu, Mińsku Mazowieckim, Nowym Targu i Świnoujściu.

[114] UM w Mińsku Mazowieckim.

[115] UM w: Andrychowie, Głogowie, Dąbrowie Górniczej, Koszalinie, Mikołowie, Mińsku Mazowieckim, Mysłowicach, Legnicy, Lesznie, Ostrowie Wlkp., Płocku, Pruszkowie, Radomiu, Śremie, Świdnicy i Stargardzie Szczecińskim.

teleinformatycznego, obowiązujących procedur ustanowionych w Polityce Bezpieczeństwa Informacji oraz komunikacji w sieci komputerowej. Szkolenia prowadzone były zarówno przez pracowników urzędów, np. przez Pełnomocnika ds. Informacji Niejawnych, Administratora Bezpieczeństwa Informacji, jak i przez firmy zewnętrzne. W szkoleniach brali udział zarówno informatycy, jak i pracownicy, którzy posiadali dostęp do systemów informatycznych.

- *Przykładem właściwie zorganizowanego procesu szkoleń w ww. zakresie jest **Urząd Miasta w Legnicy**, w którym szkolenia miały charakter usystematyzowany i odbywały się według ściśle określonych harmonogramów w roku. Ponadto, w ramach polityki bezpieczeństwa w okresie objętym kontrolą z Referatu Informatyki wysyłane były, droga mailową zasady i informacje dotyczące prawidłowej eksploatacji systemów informatycznych i zabezpieczeń, w tym m.in.:*
  – poczty elektronicznej,
  – dodawania i usuwania informacji na stronach internetowych,
  – pracy użytkowników z systemami,
  – sprawdzania systemów programem antywirusowym.
- *Innym przykładem pozytywnego działania w omawianym zakresie jest **Urząd Miasta Płocka**, w którym w okresie od dnia 31 maja 2012 r. do 9 czerwca 2014 r. zorganizowano pięć szkoleń m.in. z zakresu bezpieczeństwa informacji, w których udział wzięło łącznie 1202 pracowników (przy zatrudnieniu wahającym się od 608 do 698 pracowników). Szkolenia uwzględniały takie zagadnienia jak: obowiązujące regulacje dotyczące zasad bezpieczeństwa informacji, przykłady zagrożeń bezpieczeństwa informacji wynikających z podatności czynnika ludzkiego. Ponadto każdy nowy pracownik był zobowiązany do zapoznania się i stosowania instrukcji podstawowych zasad bezpieczeństwa informacji dla pracowników Urzędu Miasta Płocka.*

Uwagi NIK dotyczyły jednego urzędu[116], w którym przeprowadzone szkolenia z zakresu bezpieczeństwa informacji pracowników miały wyłącznie charakter jednorazowy i odbywały się tylko w momencie rozpoczęcia zatrudnienia. NIK zwróciła uwagę, że, szkolenia w zakresie zagrożeń bezpieczeństwa informacji oraz skutków ich naruszenia powinny się odbywać w ustalonych odstępach czasowych ze względu na szybko zachodzące zmiany w zakresie bezpieczeństwa przetwarzania danych w systemach informatycznych.

W pozostałych siedmiu jednostkach[117] (tj. 29,2%) po 31 maja 2012 r., tj. po wejściu w życie rozporządzenia KRI, nie przeprowadzono szkoleń w zakresie bezpieczeństwa informacji, w związku z tym NIK wnioskowała o ich przeprowadzenie[118]. W odpowiedziach na wystąpienia pokontrolne kierownicy skontrolowanych jednostek poinformowali o przyjęciu wniosku do realizacji i podjętych w tym zakresie działaniach.

Zdaniem NIK istnieje potrzeba, aby pracownicy zaangażowani w proces przetwarzania informacji zostali przeszkoleni oraz byli regularnie powiadamiani o zagrożeniach w obszarze bezpieczeństwa informacji, a także o zmianach w zakresie obowiązujących w urzędzie polityk i procedur związanych z wykonywanymi przez nich zadaniami. Zwiększy to świadomość pracowników co do występujących zagrożeń związanych z bezpieczeństwem informacji.

3.3.6. Praca na odległość i mobilne przetwarzanie danych

W § 20 ust. 2 pkt 8 rozporządzenia KRI wskazano na konieczność ustanowienia podstawowych zasad gwarantujących bezpieczną pracę przy przetwarzaniu mobilnym i pracy na odległość.

W 11 urzędach[119] (45,8%) ustanowiono podstawowe zasady bezpiecznej pracy użytkowników przy wykorzystaniu komputerów przenośnych. Zasady określały m.in. sposoby zabezpieczenia urządzeń mobilnych (laptopy, tablety, smartfony) i danych w nich zawartych przed kradzieżą

[116] UM w Zawierciu.

[117] UM w: Chrzanowie, Dzierżoniowie, Luboniu, Nowym Targu, Olkuszu, Szczecinku i Świnoujściu.

[118] Za wyjątkiem UM Nowy Targ, w którym szkolenia prowadzone były w trakcie kontroli.

[119] UM w: Dąbrowie Górniczej, Legnicy, Lesznie, Luboniu, Mysłowicach, Ostrowie Wlkp., Płocku, Radomiu, Szczecinku, Świdnicy i Zawierciu.

i nieuprawnionym dostępem poza siedzibą jednostki, a także zasady korzystania z ogólnodostępnych sieci bezprzewodowych oraz aktualizacji oprogramowania urządzeń przenośnych.

W 13 urzędach[120] (54,2%) nie ustanowiono zasad (procedur) gwarantujących bezpieczną pracę przy przetwarzaniu mobilnym i pracy na odległość, co było niezgodne z § 20 ust. 2 pkt 8 rozporządzenia KRI. W siedmiu urzędach[121] jako przyczynę nieopracowania i niewdrożenia procedur bezpiecznej pracy na urządzeniach mobilnych poza urzędem wskazywano m.in., że nie wykorzystywano urządzeń do pracy poza urzędem, jak również brak możliwości realizowania zdalnie zadań z wykorzystaniem systemów informatycznych jednostki. Jakkolwiek NIK nie formułowała w tych przypadkach wniosków o opracowanie takich procedur, to jednak jest zdania, że **podstawową funkcją urządzeń mobilnych, takich jak posiadane przez urzędy laptopy jest praca w dowolnym miejscu z wykorzystaniem technik komunikacyjnych. A zatem nie można wykluczyć, że praca może być niekiedy wykonywana również poza siedzibą urzędu, co powoduje szereg zagrożeń dla bezpieczeństwa danych zapisanych w tych urządzeniach (np. kradzież, modyfikacja danych).**

W pozostałych sześciu urzędach, procedury dotyczące bezpiecznej pracy przy przetwarzaniu mobilnym i pracy na odległość zostały opracowane w trakcie kontroli lub, jak poinformowali kontrolowani, zostaną opracowane.

3.3.7. Serwis sprzętu informatycznego i oprogramowania

Przepis § 20 ust. 2 pkt 10 rozporządzenia KRI zobowiązują do zawierania w umowach serwisowych podpisanych ze stronami trzecimi zapisów gwarantujących odpowiedni poziom bezpieczeństwa informacji.

Kontrola wykazała, że w 16 urzędach (66,7%) we wszystkich umowach na zakup lub serwis sprzętu komputerowego/oprogramowania wybranych do kontroli systemów informatycznych zawarto zapisy o zobowiązaniu wykonawców umów do zachowania w tajemnicy informacji, do jakich może mieć dostęp w związku z realizowaniem umowy.

W umowach zakupu, zapisy dotyczące serwisu gwarancyjnego stanowiły, że w przypadku uszkodzenia dysków twardych, pozostaną one w dyspozycji urzędów i nie będą zwracane do producenta sprzętu. W przypadku serwisu po gwarancji, wydawano do naprawy sprzęt komputerowy bez dysku twardego, bądź dokonywano naprawy sprzętu w siedzibie urzędu.

W pozostałych ośmiu urzędach (33,3%) w umowach na zakup lub serwis sprzętu komputerowego/ /oprogramowania wybranych do kontroli systemów informatycznych stwierdzono brak zapisów gwarantujących zabezpieczenie poufności informacji uzyskanych przez wykonawców w związku z realizacją tych umów, co było niezgodne z § 20 ust. 2 pkt 10 rozporządzenia KRI. Zapisów takich nie zawarto łącznie w 28[122] umowach spośród 63 objętych badaniem (44,4%).

Kontrolowani podawali m.in., że zapisów takich nie zawierano gdyż zasady zachowania w tajemnicy informacji przetwarzanych w systemach informatycznych zostały ustalone „nieformalnie", jak też wskazywali, że kwestie te są uregulowane w PBI, a zawarcie takich postanowień w umowie powoduje wzrost ceny zakupu sprzętu.

[120] UM w: Andrychowie, Chrzanowie, Dzierżoniowie, Głogowie, Koszalinie, Mikołowie, Mińsku Mazowieckim, Nowym Targu, Pruszkowie, Olkuszu, Stargardzie Szczecińskim, Śremie i Świnoujściu.

[121] UW w: Andrychowie, Koszalinie, Mińsku Mazowieckim, Nowym Targu, Olkuszu, Pruszkowie i Śremie.

[122] UM w (liczba umów bez właściwych zapisów/liczba zbadanych umów): Dzierżoniowie (3/6), Głogowie (4/13), Lesznie (1/1), Nowym Targu (2/6), Olkuszu (5/22), Pruszkowie (4/4), Śremie (4/4) i Świnoujściu (5/7).

Zdaniem NIK, uzgodnienia nieformalne bez wprowadzenia odpowiednich zapisów w umowach nie zabezpieczają należycie interesów zamawiającego i pozbawiają go możliwości skutecznego dochodzenia odpowiedzialności usługodawcy w przypadku niedochowania uzgodnień. Stosowanie takich postanowień w umowach jest powszechne w obrocie gospodarczym, a same zasady określone w PBI nie gwarantują odpowiedniego zabezpieczenia informacji w relacjach z wykonawcą usług serwisowych.

3.3.8. Procedury zgłaszania incydentów naruszenia bezpieczeństwa informacji

Zgodnie z § 20 ust. 2 pkt 13 rozporządzenia KRI, zarządzanie bezpieczeństwem informacji realizowane jest m.in. poprzez bezzwłoczne zgłaszanie incydentów naruszenia bezpieczeństwa informacji w określony i z góry ustalony sposób, umożliwiający szybkie podjęcie działań korygujących.

W 23 urzędach[123] (95,8%) opracowano i wdrożono procedury regulujące zasady postępowania w przypadku wystąpienia incydentów naruszenia bezpieczeństwa informacji, jednakże w 17 urzędach[124] procedury te odnosiły się tylko do przypadków zaistnienia incydentów związanych z przetwarzaniem danych osobowych. W sześciu urzędach[125] opracowano dokumenty wskazujące pracownikom sposób zachowania w przypadku stwierdzenia zdarzenia mogącego mieć wpływ na bezpieczeństwo przetwarzania informacji w urzędzie. Na przykład:

- *W **Urzędzie Miejskim w Dąbrowie Górniczej** obowiązywała Instrukcja postępowania w sytuacji naruszenia bezpieczeństwa informacji. Odnosiła się do wszelkich mogących mieć miejsce zdarzeń lub działań niezamierzonych, które stanowią lub mogły stanowić przyczynę utraty zasobów, zmian poufności, integralności, dostępności informacji lub niezawodności systemów, a także odstępstw od obowiązujących procedur postępowania, nawet jeżeli nie prowadzą do ww. skutków.*

Zdaniem NIK procedury zgłaszania incydentów naruszenia bezpieczeństwa informacji powinny dotyczyć zarówno zgłaszania zagrożeń w zakresie danych osobowych, jak i innych informacji przetwarzanych w urzędzie. Stosowanie procedur określonych tylko dla danych osobowych może ograniczać ilość informacji o zagrożeniach jakie winny być zgłaszane przez pracowników w związku z wystąpieniem niepożądanych zdarzeń przy przetwarzaniu informacji innych, niż dane osobowe.

3.3.9. Audyt wewnętrzny z zakresu bezpieczeństwa informacji

W myśl § 20 ust. 2 pkt 14 rozporządzenia KRI, zarządzanie bezpieczeństwem informacji realizowane jest m.in. poprzez zapewnienie przez kierownictwo podmiotu publicznego warunków umożliwiających realizację i egzekwowanie działania polegającego na okresowym audycie wewnętrznym w zakresie bezpieczeństwa informacji, nie rzadziej niż raz na rok.

W okresie objętym kontrolą w dziewięciu[126] urzędach (tj. 37,5%) nie przeprowadzono audytu w zakresie bezpieczeństwa informacji w systemach informatycznych. Powyższą nieprawidłowość tłumaczono m.in. faktem, że audyt o podobnej tematyce został przeprowadzony w latach wcześniejszych, a także brakiem pracowników posiadających niezbędną wiedzę i doświadczenie dla przeprowadzenia takiego audytu. W trakcie kontroli, bądź w odpowiedziach na wystąpienia pokontrolne, kontrolowani zadeklarowali przeprowadzenie audytu bezpieczeństwa informacji w ostatnim kwartale 2014 r.

---

123 W Urzędzie Miasta Nowy Targ nie wprowadzono do stosowania procedur zgłaszania incydentów naruszenia bezpieczeństwa informacji.

124 UM w: Chrzanowie, Andrychowie, Dzierżoniowie, Koszalinie, Lesznie, Luboniu, Olkuszu, Ostrów Wlkp., Szczecinku, Mikołowie, Mińsku Mazowieckim, Mysłowicach, Pruszkowie, Radomiu, Stargardzie Szechińskim, Świnoujściu i Zawierciu.

125 UM w: Dąbrowie Górniczej, Głogowie, Legnicy, Płocku, Śremie i Świdnicy.

126 UM w: Andrychowie, Głogowie, Lesznie, Olkuszu, Pruszkowie, Stargardzie Szczecińskim, Szczecinku, Świnoujściu i Zawierciu.

W 15 jednostkach przeprowadzono coroczny audyt bezpieczeństwa informacji. Audytorzy formułowali zalecenia – rekomendacje, które dotyczyły m.in.:

- zaktualizowania obowiązującej Polityki Bezpieczeństwa Informacji,
- dokonywania zmiany lub odbierania pracownikom uprawnień dostępu do systemów informatycznych w przypadku zmiany lub ustania wykonywanych przez nich zadań,
- opracowania procedury postępowania z incydentami naruszenia bezpieczeństwa informacji,
- wprowadzania w umowach serwisowych zapisów gwarantujących odpowiedni poziom bezpieczeństwa informacji.

3.3.10. Kopie zapasowe

Zgodnie z wymogami określonymi w § 20 ust. 2 pkt 12 lit. b rozporządzenia KRI, zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez zapewnienie przez kierownictwo podmiotu publicznego warunków umożliwiających realizację i egzekwowanie m.in. zapewnienia odpowiedniego poziomu bezpieczeństwa w systemach teleinformatycznych, polegającego w szczególności na minimalizowaniu ryzyka utraty informacji w wyniku awarii.

W 20 kontrolowanych urzędach (83,3%) kopie zapasowe danych były właściwie tworzone, przechowywane oraz testowane. W czterech urzędach (16,7%) stwierdzono nieprawidłowości polegające na niespełnieniu wymogów wynikających z § 20 ust. 2 pkt 12 lit. b, które polegały na:

- niewłaściwym przechowywaniu kopii zapasowych danych z systemów informatycznych, tj. w sposób, który nie minimalizuje ryzyka utraty informacji i stwarza zagrożenie, że w przypadku zdarzeń losowych, np. pożaru lub zalania, urząd może utracić zarówno dane źródłowe, jak i ich kopie zapasowe[127]. Stwierdzono, że sporządzane kopie zapasowe przechowywane były w serwerowniach, a więc w miejscach wytwarzania danych. Zgodnie z pkt 10.5.1 lit. d normy PN-ISO/IEC 17799:2007 kopie zapasowe powinny być przechowywane w innej lokalizacji niż miejsce ich tworzenia, w odległości niezbędnej do uniknięcia uszkodzeń spowodowanych przez katastrofę, która dotknęła ośrodek podstawowy;
- braku właściwego zabezpieczenia dostępu do przechowywanych kopii zapasowych, który nie gwarantował, że dostęp do nich posiadać będą jedynie uprawnione osoby[128],
- nie testowaniu kopii zapasowych w jednym urzędzie[129] w przypadku dwóch z trzech badanych systemów informatycznych. Zgodnie z pkt 10.5.1 lit. f normy PN-ISO/IEC 17799:2007 nośniki kopii zapasowych winny być testowane aby można było na nich polegać w przypadku awaryjnego odtwarzania.

3.3.11. Format danych udostępniany przez badane systemy informatyczne

W § 18 ust. 1 rozporządzenia KRI określono warunek udostępnienia zasobów informacyjnych co najmniej w jednym z formatów wymienionych w załączniku nr 2 do tego rozporządzenia KRI.

Wszystkie objęte badaniem 79 systemy informatyczne udostępniały zasoby informatyczne co najmniej w jednym formacie wymienionym w załączniku Nr 2 do rozporządzenia KRI. Tym samym spełniony został warunek określony w przywołanym wyżej przepisie rozporządzeniu KRI.

[127] UM w: Luboniu, Mińsku Mazowieckim, Nowym Targu.
[128] UM w Luboniu i Pruszkowie.
[129] UM w Pruszkowie.

Stwarzało to możliwość wymiany danych pomiędzy różnymi systemami informatycznymi oraz pozwalało odbiorcom na swobodny dostęp do informacji poprzez wygenerowanie danych w powszechnie znanych i dostępnych plikach.

3.4 Zapewnienie dostępności informacji zawartych na stronach internetowych urzędów dla osób niepełnosprawnych

Zgodnie z § 19 rozporządzenia KRI, w ramach dostosowania systemów prezentujących treści do wymagań Web Content Accessibility Guidelines (WCAG 2.0[130]), powinno nastąpić ich dostosowanie do potrzeb osób niepełnosprawnych, uwzględniając poziom AA, określony w załączniku nr 4 do rozporządzenia KRI. Najwyższa Izba Kontroli nie dokonywała oceny działalności kontrolowanych urzędów w tym obszarze, gdyż zgodnie z § 22 rozporządzenia KRI systemy teleinformatyczne podmiotów realizujących zadania publiczne należy dostosować do wymagań określonych w § 19 rozporządzenia KRI, nie później niż w terminie 3 lat od dnia wejścia w życie rozporządzenia, czyli do 31 maja 2015 r.

Weryfikację zgodności stron internetowych i BIP kontrolowanych urzędów, pod kątem spełnienia wymogów prezentacji zasobów informacyjnych zgodnie ze standardem WCAG 2.0 w zakresie Zasady 4 – Kompatybilność przeprowadzono za pomocą narzędzi dostępnych na stronie http://validator.w3.org oraz http://jigsaw.w3.org/css-validator.

Kontrola wykazała, że strony internetowe i BIP skontrolowanych urzędów w różnym stopniu zostały dostosowane do odbioru ich treści przez osoby niepełnosprawne. Stosowano rozwiązania techniczne umożliwiające osobom niedosłyszącym lub niedowidzącym zapoznanie się z treścią informacji m.in. poprzez powiększenie czcionki, obrazu, zmianę kontrastu czy też odsłuchanie wyświetlanej treści. Przeprowadzone badania z wykorzystaniem ww. narzędzi wykazały, że we wszystkich kontrolowanych urzędach na ich stronach internetowych i/lub na stronach BIP występowały błędy związane z prezentowaniem treści dla osób niepełnosprawnych. Na przykład:

- *W **Urzędzie Miasta Świnoujście** strona internetowa urzędu nie umożliwiała odsłuchania zapisu informacji.*
- *W **Urzędzie Miejskim w Zawierciu** strony internetowe urzędu umożliwiały wyświetlenie treści z powiększoną czcionką, nie zapewniały jednak możliwości zwiększenia kontrastu.*
- *W **Urzędzie Miasta Leszna** strona BIP urzędu nie posiadała żadnych funkcjonalności ułatwiających korzystanie z zamieszczonych w niej informacji osobom niepełnosprawnym.*

Niezbędne jest więc podejmowanie dalszych działań w celu wyeliminowania ujawnionych błędów i poprawy funkcjonalności stron internetowych i BIP w odbiorze przez osoby niepełnosprawne. Zaznaczyć należy, że prace takie w części urzędów prowadzone były już w trakcie kontroli, bądź deklarowano ich wykonanie i zakończenie do 31 maja 2015 r. Na przykład:

- *W **Urzędzie Miejskim w Pruszkowie** realizowana jest umowa, w ramach której do końca września 2014 r. planowano wykonanie prac dla dostawania strony internetowej urzędu dla potrzeb osób niepełnosprawnych. Trwały również prace przygotowawcze nad uruchomieniem nowego serwisu strony BIP urzędu.*
- *W **Urzędzie Miasta Nowy Targ** zaplanowano realizację obowiązku dostosowania strony internetowej i BIP do potrzeb niepełnosprawnych na IV kwartał 2014 r. i I kwartał 2015 r.*
- *W **Urzędzie Miejskim w Ostrowie Wlkp.** dokonano wyboru wykonawcy audytu dostępności strony internetowej urzędu w zakresie spełnienia przez tą stronę wymogów WCAG 2.0., co umożliwi jej modyfikację.*

[130] WCAG jest standardem służącym dostosowaniu wyświetlanej treści na stronie internetowej do potrzeb osób niedowidzących. Rozwiązanie to ma na celu zapewnienie prezentacji treści w sposób ułatwiający osobom niepełnosprawnym zapoznanie się z wiadomościami. Ułatwienia te koncentrują się na sposobie wyświetlania i komunikatach głosowych.

4 INFORMACJE DODATKOWE

4.1 Przygotowanie kontroli

Kontrolę koordynował Departament Administracji Publicznej. Czynności kontrolne zostały przeprowadzone w 25 jednostkach przez sześć jednostek organizacyjnych NIK, tj. Departament Administracji Publicznej oraz Delegatury NIK w: Katowicach, Krakowie, Poznaniu, Szczecinie i we Wrocławiu.

4.2 Postępowanie kontrolne i działania podjęte po zakończeniu kontroli

Postępowanie kontrolne przeprowadzono w 25 jednostkach. Najwyższa Izba Kontroli skierowała 25 wystąpień pokontrolnych do wszystkich kierowników kontrolowanych jednostek. Z danych na dzień 16 stycznia 2015 r. wynika, że na 84 wnioski pokontrolne sformułowane przez NIK, 30 zostało zrealizowanych, 54 było w trakcie realizacji. W trzech wystąpieniach pokontrolnych zostały zawarte ogólne oceny pozytywne, a w 22 oceny opisowe wskazujące na działania realizowane prawidłowo oraz na stwierdzone nieprawidłowości. Do wystąpień pokontrolnych nie zgłoszono zastrzeżeń.

Wnioski skierowane do Ministra Administracji i Cyfryzacji dotyczyły:

- uwzględnienia w planach kontroli Ministerstwa i realizowania kontroli w podmiotach publicznych w zakresie działania systemów teleinformatycznych, prowadzenia rejestrów i wymiany informacji w postaci elektronicznej oraz podjęciu działań w celu pozyskania specjalistów posiadających odpowiednie kwalifikacje do przeprowadzenia takich kontroli,
- przeprowadzenia prac koniecznych dla zrealizowania zadań krótkookresowych dotyczących interoperacyjności określonych w pkt 6.3.1 *Programu Zintegrowanej Informatyzacji Państwa*.

Wnioski skierowane do burmistrzów/prezydentów miast dotyczyły m.in.:

- przekazania do CRD wzorów dokumentów elektronicznych świadczonych usług elektronicznych,
- aktualizacji strony BIP urzędu poprzez umieszczenie na niej informacji odnośnie obowiązujących procedur w zakresie załatwiania spraw drogą elektroniczną,
- opracowania i wdrożenia Polityki Bezpieczeństwa Informacji, określającej zasady bezpieczeństwa informacji, zgodnej z normą PN-ISO/IEC 27001,
- prowadzenia aktualnej i kompletnej inwentaryzacji sprzętu informatycznego obejmującej jego rodzaj i konfigurację,
- odebrania użytkownikom systemów informatycznych niebędących pracownikami służb informatycznych uprawnień umożliwiających instalowanie oprogramowania,
- niezwłocznego blokowania dostępu do systemów informatycznych byłym pracownikom urzędu,
- wyeliminowania możliwości zalogowania się do systemów informatycznych bez podania hasła dostępu,
- przeszkolenia wszystkich osób zaangażowanych w proces przetwarzania informacji w zakresie zachowania bezpieczeństwa informacji,
- opracowania i wdrożenia procedur gwarantujących bezpieczną pracę przy przetwarzaniu mobilnym i pracy na odległość,
- opracowania i wdrożenia zasad określających sposób zgłaszania incydentów naruszenia bezpieczeństwa informacji,

– zawierania w umowach serwisowych zapisów gwarantujących odpowiedni poziom bezpieczeństwa informacji,
– przeprowadzania okresowych audytów w zakresie bezpieczeństwa informacji nie rzadziej niż raz na rok,
– przechowywania kopii zapasowych systemów informatycznych i danych w nich zawartych, poza serwerownią w miejscu właściwie zabezpieczonym przed dostępem osób nieupoważnionych i zdarzeniami losowymi.

Adresaci wystąpień pokontrolnych poinformowali o podjęciu działań na rzecz realizacji wniosków pokontrolnych. Na przykład:

- *Burmistrz Miasta i Gminy Olkusz poinformował m.in., że: do 31 grudnia 2014 r. opracowana zostanie Polityka Bezpieczeństwa Informacji i wdrożona w I kwartale 2015 r.; audyty w zakresie bezpieczeństwa informacji będą wykonywane corocznie; podjęto prace dla zmiany uprawnień pracowników do systemów informatycznych urzędu oraz zaktualizowania kart informacyjnych komputerów. Poinformował również, że w 2015 r. planowany jest zakup oprogramowania, który będzie zawierał moduł do zarządzania zasobami informatycznymi.*
- *Prezydent Miasta Świnoujście poinformował m.in., że: trwają prace nad opracowaniem Polityki Bezpieczeństwa Informacji, której wdrożenie nastąpi do 31 stycznia 2015 r. Obejmować ona będzie również procedurę tworzenia i przechowywania kopii zapasowych danych przetwarzanych w systemach informatycznych. Poinformował również, że przeprowadzona zostanie inwentaryzacja sprzętu komputerowego, a jej zakończenie nastąpi 31 marca 2015 r., w umowach serwisowych na 2015 r. zostaną zawarte zapisy gwarantujące zabezpieczenie poufności informacji oraz że podjęte zostaną działania mające na celu popularyzacji wśród obywateli komunikacji elektronicznej z Urzędem.*
- *Prezydent Miasta Pruszkowa poinformował m.in., że: wykonano kompletną inwentaryzację sprzętu komputerowego obejmującą jego rodzaj i konfigurację; odebrano użytkownikom systemów informatycznym niebędącymi pracownikami służb informatycznych uprawnienia umożliwiające instalowanie oprogramowania, dostosowano nowe pomieszczenie do przechowywania kopii zapasowych danych przetwarzanych w systemach informatycznych oraz określono terminy testowania kopii zapasowych.*

Minister Administracji i Cyfryzacji w odpowiedzi na wystąpienie pokontrolne poinformował m.in., że:

– w celu przeprowadzania kontroli w podmiotach publicznych w zakresie działania systemów teleinformatycznych, prowadzenia rejestrów i wymiany informacji w postaci elektronicznej podjęto działania dla pozyskania pracownika posiadającego wymagane kwalifikacje (certyfikaty), a także skieruje kolejnego na szkolenie/studia podyplomowe, kończące się uzyskaniem certyfikatu,
– podejmie wszelkie niezbędne działania mające na celu właściwą realizację zadań określonych w pkt 6.3.1. *Programu Zintegrowanej Informatyzacji Państwa*.

Charakterystyka uwarunkowań oraz stanu prawnego

Interoperacyjność w jednostkach świadczących usługi publiczne

Zgodnie z art. 13 ust. 1 ustawy o informatyzacji, podmiot publiczny używa do realizacji zadań publicznych systemów teleinformatycznych spełniających minimalne wymagania dla systemów teleinformatycznych oraz zapewniających interoperacyjność systemów na zasadach określonych w Krajowych Ramach Interoperacyjności. Na podstawie upoważnienia zawartego w art. 18 tej ustawy, rozporządzenie KRI określa Krajowe Ramy Interoperacyjności, minimalne wymagania dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalne wymagania dla systemów teleinformatycznych.

Zgodnie z § 4 ust. 1 rozporządzenia KRI, interoperacyjność osiąga się przez:

- ujednolicenie, rozumiane jako zastosowanie kompatybilnych norm, standardów i procedur przez różne podmioty realizujące zadania publiczne, lub
- wymienność, rozumianą jako możliwość zastąpienia produktu, procesu lub usługi bez jednoczesnego zakłócenia wymiany informacji pomiędzy podmiotami realizującymi zadania publiczne lub pomiędzy tymi podmiotami a ich klientami, przy jednoczesnym spełnieniu wszystkich wymagań funkcjonalnych i poza funkcjonalnych współpracujących systemów, lub
- zgodność, rozumianą jako przydatność produktów, procesów lub usług przeznaczonych do wspólnego użytkowania, pod specyficznymi warunkami zapewniającymi spełnienie istotnych wymagań i przy braku niepożądanych oddziaływań.

Zastosowanie reguł określonych w ww. ust. 1 zależne jest od okoliczności wynikających z szacowania ryzyka oraz z właściwości projektowanego systemu teleinformatycznego, jego zasięgu oraz dostępnych rozwiązań na rynku dostaw i usług w zakresie informatyki (§ 4 ust. 2). Zastosowany przez podmiot realizujący zadania publiczne sposób osiągnięcia interoperacyjności nie może naruszać zasady neutralności technologicznej[131] (§ 4 ust. 3).

Zgodnie z § 5 ust. 1 rozporządzenia KRI, podmioty realizujące zadania publiczne stosują rozwiązania z zakresu interoperacyjności na poziomie organizacyjnym, semantycznym i technologicznym. Interoperacyjność na poziomie organizacyjnym osiągana jest przez (§ 5 ust. 2):

1) informowanie przez podmioty realizujące zadania publiczne, w sposób umożliwiający skuteczne zapoznanie się, o sposobie dostępu oraz zakresie użytkowym serwisów dla usług realizowanych przez te podmioty;
2) wskazanie przez ministra właściwego do spraw informatyzacji miejsca przeznaczonego do publikacji informacji, o których mowa w pkt 1;
3) standaryzację i ujednolicenie procedur z uwzględnieniem konieczności zapewnienia poprawnej współpracy podmiotów realizujących zadania publiczne;
4) publikowanie i uaktualnianie w Biuletynie Informacji Publicznej przez podmiot realizujący zadania publiczne opisów procedur obowiązujących przy załatwianiu spraw z zakresu jego właściwości drogą elektroniczną.

[131] W ustawie o informatyzacji (art. 3 pkt 19) zdefiniowano znaczenie terminu zasady neutralności technologicznej, zgodnie z którym jest to zasada równego traktowania przez władze publiczne technologii teleinformatycznych i tworzenia warunków do ich uczciwej konkurencji, w tym zapobiegania możliwości eliminacji technologii konkurencyjnych przy rozbudowie i modyfikacji eksploatowanych systemów teleinformatycznych lub przy tworzeniu konkurencyjnych produktów i rozwiązań.

Interoperacyjność na poziomie semantycznym osiągana jest przez (§ 5 ust. 3):

1) stosowanie struktur danych i znaczenia danych zawartych w tych strukturach, określonych w niniejszym rozporządzeniu;
2) stosowanie struktur danych i znaczenia danych zawartych w tych strukturach publikowanych w repozytorium interoperacyjności na podstawie przepisów § 8 ust. 3 oraz § 10 ust. 5, 6, 11 i 12 rozporządzenia KRI;
3) stosowanie w rejestrach prowadzonych przez podmioty publiczne odwołań do rejestrów zawierających dane referencyjne w zakresie niezbędnym do realizacji zadań.

Interoperacyjność na poziomie technologicznym osiągana jest przez (§ 5 ust. 4):

1) stosowanie minimalnych wymagań dla systemów teleinformatycznych, określonych w rozdziale IV rozporządzenia KRI;
2) stosowanie regulacji zawartych w przepisach odrębnych, a w przypadku ich braku uwzględnienia postanowień odpowiednich Polskich Norm, norm międzynarodowych lub standardów uznanych w drodze dobrej praktyki przez organizacje międzynarodowe.

Systemy informatyczne służące realizacji zadań publicznych, w myśl § 8 ust. 1 rozporządzenia KRI, powinny stosować rozwiązania oparte na modelu usługowym[132].

Organizacja bezpieczeństwa informacji

W myśl § 15 ust. 1 rozporządzenia KRI, systemy teleinformatyczne używane przez podmioty realizujące zadania publiczne projektuje się, wdraża oraz eksploatuje z uwzględnieniem ich funkcjonalności, niezawodności, używalności, wydajności, przenoszalności i pielęgnowalności, przy zastosowaniu norm oraz uznanych w obrocie profesjonalnym standardów i metodyk.

Zarządzanie usługami realizowanymi przez systemy teleinformatyczne ma na celu dostarczanie tych usług na deklarowanym poziomie dostępności i odbywa się w oparciu o udokumentowane procedury (§ 15 ust. 2). Wymagania określone w ust. 1 i 2 uznaje się za spełnione, jeśli projektowanie, wdrażanie, eksploatowanie, monitorowanie, przeglądanie, utrzymanie i udoskonalanie zarządzania usługą podmiotu realizującego zadanie publiczne odbywają się z uwzględnieniem Polskich Norm: PN-ISO/IEC 20000-1 i PN-ISO/IEC 20000-2 (§ 15 ust. 3).

Zgodnie z załącznikiem Nr 2 do rozporządzenia KRI, system teleinformatyczny używany do realizacji zadań publicznych musi obsługiwać standardy zapewniające dostęp do zasobów informacji oraz formaty danych określone w załączniku.

Podmiot realizujący zadania publiczne opracowuje i ustanawia, wdraża i eksploatuje, monitoruje i przegląda oraz utrzymuje i doskonali system zarządzania bezpieczeństwem informacji zapewniający poufność, dostępność i integralność informacji z uwzględnieniem takich atrybutów, jak autentyczność, rozliczalność, niezaprzeczalność i niezawodność (§ 20 ust. 1 rozporządzenia KRI).

Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności poprzez zapewnienie przez kierownictwo podmiotu publicznego warunków umożliwiających realizację i egzekwowanie działań wymienionych § 20 ust. 2 rozporządzenia KRI, w tym m.in. zapewnienie:

[132] Model usługowy jest modelem architektury systemu informatycznego, w którym dla użytkowników zdefiniowano stanowiące odrębną całość funkcje systemu teleinformatycznego (usługi sieciowe) oraz opisano sposób korzystania z tych funkcji.

- aktualizacji regulacji wewnętrznych w zakresie dotyczącym zmieniającego się otoczenia (pkt 1),
- utrzymywania aktualności inwentaryzacji sprzętu i oprogramowania służącego do przetwarzania informacji obejmującej ich rodzaj i konfigurację (pkt 2),
- przeprowadzania okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji oraz podejmowania działań minimalizujących to ryzyko, stosownie do wyników przeprowadzonej analizy (pkt 3),
- podejmowania działań zapewniających, że osoby zaangażowane w proces przetwarzania informacji posiadają stosowne uprawnienia i uczestniczą w tym procesie w stopniu adekwatnym do realizowanych przez nie zadań oraz obowiązków mających na celu zapewnienie bezpieczeństwa informacji (pkt 4),
- bezzwłocznej zmiany uprawnień w przypadku zmiany zadań (pkt 5),
- zapewnienia szkolenia osób zaangażowanych w proces przetwarzania informacji (pkt 6),
- ustanowienia podstawowych zasad gwarantujących bezpieczną pracę przy przetwarzaniu mobilnym i pracy na odległość (pkt 8),
- ustalenia zasad postępowania z informacjami, zapewniających minimalizację wystąpienia ryzyka kradzieży informacji i środków przetwarzania informacji, w tym urządzeń mobilnych (pkt 11),
- zapewnienia odpowiedniego poziomu bezpieczeństwa w systemach teleinformatycznych, polegającego w szczególności na: minimalizowaniu ryzyka utraty informacji w wyniku awarii, zapewnieniu bezpieczeństwa plików systemowych, kontroli zgodności systemów teleinformatycznych z odpowiednimi normami i politykami bezpieczeństwa (pkt 12 lit. b, e, h),
- zapewnienia okresowego audytu wewnętrznego w zakresie bezpieczeństwa informacji, nie rzadziej niż raz na rok (pkt 14).

Zgodnie z § 20 ust. 3 rozporządzenia KRI, obowiązki, o których mowa w § 20 ust. 1 i 2 uznaje się za spełnione, jeżeli system zarządzania bezpieczeństwem informacji został opracowany na podstawie Polskiej Normy PN-ISO/IEC 27001, a ustanawianie zabezpieczeń, zarządzanie ryzykiem oraz audytowanie odbywa się na podstawie Polskich Norm związanych z tą normą, w tym: PN-ISO/IEC 17799 – w odniesieniu do ustanawiania zabezpieczeń; PN-ISO/IEC 27005 – w odniesieniu do zarzadzania ryzykiem; PN-ISO/IEC 24762 – w odniesieniu do odtwarzania techniki informatycznej po katastrofie w ramach zarządzania ciągłością działania.

W kwestii dotyczącej zapewnienia okresowego audytu wewnętrznego w zakresie bezpieczeństwa informacji, o którym mowa w § 20 ust. 2 pkt 14 rozporządzenia KRI, Departament Informatyzacji MAiC oraz Departament Audytu Sektora Finansów Publicznych Ministerstwa Finansów opracowały wspólne stanowisko w powyższym zakresie[133]. Prezentuje ono dwa sposoby wywiązania się z obowiązku zapewnienia okresowego audytu w zakresie bezpieczeństwa informacji. W stanowisku tym podano m.in., że nie należy automatycznie przypisywać zadania audytu w zakresie bezpieczeństwa informacji komórce audytu wewnętrznego, oraz że punktem odniesienia dla ustanowienia niniejszych przepisów był dla projektodawcy System Zarządzania Bezpieczeństwem Informacji w oparciu o normę PN-ISO/IEC 27001, nie zaś Dział VI ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych[134]. W stanowisku stwierdzono, że intencją

[133] Źródło: strona internetowa Ministerstwa Finansów (http://www.mf.gov.pl/pl/ministerstwo-finansow/wiadomosci/aktualnosci/-/asset_publisher/M1vU/content/id/3812517).

[134] Dz. U. z 2013 r., poz. 885 ze zm.

autorów rozporządzenia w sprawie systemów teleinformatycznych było zobowiązanie podmiotów realizujących zadania publiczne do realizowania okresowego audytu wewnętrznego, bez szczegółowego wskazywania na rodzaj audytu oraz tryb jego przeprowadzania. Uwzględniając przepis § 20 ust. 3 rozporządzenia KRI, obowiązek ten może być realizowany w jeden z dwóch sposobów:

1) w podmiotach, w których system zarządzania bezpieczeństwa informacji został opracowany na podstawie Polskiej Normy PN-ISO/IEC 27001, wymagania określone w § 20 ust. 1 i 2 uznaje się za spełnione – w takich podmiotach nie ma konieczności dokonywania dodatkowych audytów wewnętrznych, gdyż audytowanie jest jednym z już funkcjonujących elementów systemu zarządzania bezpieczeństwa informacji określonym w normach,
2) jednostki, które nie opracowały i nie wdrożyły systemu bezpieczeństwa informacji, opierając się na Polskiej Normie PN-ISO/IEC 27001, są zobowiązane do zapewnienia okresowego audytu wewnętrznego w tym zakresie, nie rzadziej niż raz w roku.

W § 23 rozporządzenia KRI wskazano, że systemy teleinformatyczne podmiotów realizujących zadania publiczne funkcjonujące w dniu wejścia w życie rozporządzenia KRI należy dostosować do wymagań określonych w rozdziale IV rozporządzenia KRI (minimalne wymagania dla systemów teleinformatycznych), nie później niż w dniu ich pierwszej istotnej modyfikacji przypadającej po wejściu w życie tego rozporządzenia[135].

Dostosowanie serwisów WWW przeznaczonych dla klienta urzędu do potrzeb osób niepełnosprawnych

Zgodnie z § 19 rozporządzenia KRI, w ramach dostosowania systemów prezentujących treści do wymagań Web Content Accessibility Guidelines (WCAG 2.0) nastąpi ich dostosowanie do potrzeb osób niepełnosprawnych, uwzględniając poziom AA, określony w załączniku nr 4 do rozporządzenia KRI. W § 22 rozporządzenia KRI wskazano, iż systemy teleinformatyczne realizujące zadania publiczne funkcjonujące w dniu wejścia w życie rozporządzenia, należy dostosować do wymagań określonych w § 19, nie później niż w terminie 3 lat od wejścia w życie KRI, czyli do 31 maja 2015 r.

Zadania Ministra Administracji i Cyfryzacji

W art. 19b ust 1 i 2 ustawa o informatyzacji nakłada na ministra właściwego do spraw informatyzacji obowiązek prowadzenia w ramach ePUAP centralnego repozytorium wzorów dokumentów elektronicznych, w którym umieszcza się, przechowuje i udostępnia wzory dokumentów. Organy administracji publicznej przekazują do centralnego repozytorium oraz udostępniają w Biuletynie Informacji Publicznej wzory dokumentów elektronicznych. Przy sporządzaniu wzorów dokumentów elektronicznych stosuje się międzynarodowe standardy dotyczące sporządzania dokumentów elektronicznych przez organy administracji publicznej, z uwzględnieniem konieczności podpisywania ich bezpiecznym podpisem elektronicznym (art. 19b ust 3).

[135] Przez istotną modernizację systemu informatycznego należy rozumieć modernizację co najmniej na poziomie 10% ogólnej wartości nabycia (lub wytworzenia) systemu. Definicję taką przyjęto w oparciu m.in. o wyjaśnienie Podsekretarza Stanu w Ministerstwie Spraw Wewnętrznych i Administracji przedstawione w piśmie z dnia 10 sierpnia 2011 r. nr DSI-WPISI-0230-9-1/2011 w trakcie prac legislacyjnych nad projektem rozporządzenia KRI. W piśmie tym Podsekretarz Stanu podał m.in., że „Poprzez istotną modernizację należy rozumieć modernizację co najmniej na poziomie 10% ogólnej wartości systemu. W takiej sytuacji koszt zmiany stanowi znaczny koszt zmiany systemu." Na potrzeby niniejszej kontroli, definicja istotnej modernizacji systemu informatycznego przedstawiona przez Podsekretarza Stanu w MSWiA została uściślona przez autorów programu kontroli jako modernizacja co najmniej na poziomie 10% wartości nabycia (lub wytworzenia) systemu.

Stosownie do art. 25 ust. 1 pkt 3 lit. c ustawy o informatyzacji, minister do spraw informatyzacji dokonuje kontroli działania systemów teleinformatycznych, używanych do realizacji zadań publicznych albo realizacji obowiązków wynikających z art. 13 ust. 2 tej ustawy w podmiotach publicznych niewymienionych w lit. a i b[136] – pod względem zgodności z minimalnymi wymaganiami dla systemów teleinformatycznych lub minimalnymi wymaganiami dla rejestrów publicznych i wymiany informacji w postaci elektronicznej.

Minister Administracji i Cyfryzacji, w myśl § 9 rozporządzenia KRI zapewnia realizację publicznej dyskusji nad rekomendacjami interoperacyjności, a ponadto jest zobowiązany do prowadzenia repozytorium interoperacyjności. Dodatkowo, zgodnie z § 10 ust. 5 ww. rozporządzenia, Minister Administracji i Cyfryzacji publikuje w repozytorium interoperacyjności na ePUAP schemat XML struktury danych i cech informacyjnych obiektów.

Zgodnie z § 10 ust. 12 rozporządzenia KRI, organ władzy publicznej prowadzący rejestr publiczny zawierający inne obiekty niż wymienione w ust. 1 tego paragrafu wnioskuje do Ministra Administracji i Cyfryzacji o opublikowanie w repozytorium interoperacyjności schematu XML struktur danych cech informacyjnych tych obiektów. W repozytorium interoperacyjności, oprócz struktur danych, publikuje się także rekomendacje interoperacyjności stanowiące dobre praktyki ułatwiające osiągnięcie interoperacyjności na każdym z poziomów[137], a także zamieszcza opis protokołów i struktur wymiany danych usługi sieciowej (§ 6 i 8 ust. 3 rozporządzenia KRI).

Instrukcja kancelaryjna dla organów gminy

Zgodnie z § 1 ust. 1 rozporządzenia Prezesa Rady Ministrów z dnia 18 stycznia 2011 r. w sprawie instrukcji kancelaryjnej, jednolitych rzeczowych wykazów akt oraz instrukcji w sprawie organizacji i zakresu działania archiwów zakładowych, rozporządzenie określa m.in. instrukcję kancelaryjną dla organów gminy. W myśl § 1 załącznika nr 1 do rozporządzenia:

- czynności kancelaryjne są wykonywane w systemie tradycyjnym lub w systemie Elektronicznego Zarządzania Dokumentacją, tzw. EZD (ust. 2),
- kierownik podmiotu wskazuje, który z systemów wykonywania czynności kancelaryjnych jest podstawowym sposobem dokumentowania przebiegu załatwiania i rozstrzygania spraw dla danego podmiotu (ust. 3),
- po wskazaniu systemu EZD jako podstawowego sposobu dokumentowania przebiegu załatwiania i rozstrzygania spraw ponowne wskazanie systemu tradycyjnego jest niedopuszczalne (ust. 4),
- dokonując wyboru systemu, kierownik podmiotu może wskazać wyjątki od podstawowego sposobu dokumentowania przebiegu załatwiania i rozstrzygania spraw przez określenie klas z wykazu akt, których będą one dotyczyć, oraz wskazanie, w jakim systemie będą prowadzone (ust. 5).

ePUAP

Usługi elektroniczne świadczone dla mieszkańców mogą być realizowane przy wykorzystaniu elektronicznej platformy usług ePUAP.

Zakres i warunki korzystania z elektronicznej platformy usług administracji publicznej, w tym dotyczące: zakładania konta i sposobu prowadzenia katalogu usług na ePUAP oraz warunków wymiany informacji między ePUAP a innymi systemami teleinformatycznymi zawarte zostały

[136] W art. 25 ust. 1 pkt 3 lit a i b wymieniono: jednostki samorządu terytorialnego i ich związki oraz tworzone lub prowadzone przez te jednostki samorządowe osoby prawne i inne samorządowe jednostki organizacyjne, podmioty publiczne podległe lub nadzorowane przez organy administracji rządowej.

[137] organizacyjnym/semantycznym/technologicznym.

w rozporządzeniu Ministra Administracji i Cyfryzacji z dnia 6 maja 2014 r. w sprawie zakresu i warunków korzystania z elektronicznej platformy usług administracji publicznej, które weszło w życie z dniem 11 maja 2014 r. Poprzednio obowiązywało rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 27 kwietnia 2011 r. Za najistotniejsze, z punktu widzenia zagadnień objętych kontrolą należy wskazać wymogi dotyczące informacji o usługach elektronicznych świadczonych przez usługodawcę. Stosownie do ww. regulacji, ePUAP udostępnia katalog usług zawierający informacje o usługach, w szczególności: podstawę prawną, nazwę usługi, nazwę usługodawcy, cel usługi, odbiorców usługi, kategorie usługi oraz umiejscowienie usługodawcy według podziału administracyjnego kraju (§ 8 rozporządzenia ePUAP 6 maja 2014 r., poprzednio § 7 ust. 1 rozporządzenia ePUAP z 27 kwietnia 2011 r.). Podmioty publiczne do świadczenia usług w postaci elektronicznej mogą wykorzystywać w szczególności następujące funkcje ePUAP:

- tworzenie i obsługę dokumentów elektronicznych przez osoby fizyczne i podmioty;
- przesyłanie dokumentów elektronicznych;
- wymianę danych między ePUAP a innymi systemami teleinformatycznymi;
- identyfikację użytkowników i rozliczalność ich działań;
- weryfikację podpisu elektronicznego;
- tworzenie usług podmiotu publicznego lub kilku podmiotów publicznych współdziałających ze sobą, zbudowanych w oparciu o dwie lub więcej usług;
- obsługę płatności elektronicznych;
- potwierdzanie profilu zaufanego ePUAP (§ 9 ust. 1 rozporządzenia ePUAP z 6 maja 2014 r., poprzednio § 8 rozporządzenia ePUAP z 27 kwietnia 2011 r.).

Dostęp do informacji publicznej, w tym do informacji w BIP dla osób niepełnosprawnych

Zgodnie z art. 54 ust. 1 Konstytucji RP z dnia 2 kwietnia 1997 r.[138], każdemu zapewnia się wolność pozyskiwania i rozpowszechniania informacji. Zgodnie z art. 61 Konstytucji RP, obywatel ma prawo do uzyskiwania informacji o działalności organów władzy publicznej oraz osób pełniących funkcje publiczne. Prawo to obejmuje również uzyskiwanie informacji o działalności organów samorządu gospodarczego i zawodowego, a także innych osób oraz jednostek organizacyjnych w zakresie, w jakim wykonują one zadania władzy publicznej i gospodarują mieniem komunalnym lub majątkiem Skarbu Państwa. Prawo do uzyskiwania informacji obejmuje dostęp do dokumentów oraz wstęp na posiedzenia kolegialnych organów władzy publicznej pochodzących z powszechnych wyborów, z możliwością rejestracji dźwięku lub obrazu.

Ustawa z dnia 6 września 2001 r. o dostępie do informacji publicznej[139] określiła (art. 8) warunki udostępniania informacji publicznych w Biuletynie Informacji Publicznej. Od dnia 1 lipca 2003 r. podmioty określone w art. 4 ust. 1 ustawy są zobowiązane do udostępnienia w Biuletynie danych na temat ich statusu lub formy prawnej, organizacji, przedmiotu działalności i kompetencji, organów i osób sprawujących w nich funkcje i ich kompetencji, struktury własnościowej podmiotów wskazanych w art. 4 ust. 1 pkt 3–5 ustawy, ich majątku oraz zasad funkcjonowania. Ta ostatnia kategoria obejmuje m.in. informacje o trybie działania władz publicznych i ich jednostek organizacyjnych, trybie działania państwowych osób prawnych i osób prawnych samorządu terytorialnego w zakresie wykonywania zadań publicznych i ich działalności w ramach gospodarki budżetowej i pozabudżetowej,

[138] Dz. U. Nr 78, poz. 483 ze zm.

[139] Dz. U. z 2014 r., poz. 782.

sposobach stanowienia aktów publicznoprawnych, sposobach przyjmowania i załatwiania spraw oraz prowadzonych rejestrach, ewidencjach, archiwach oraz sposobach i zasadach udostępniania danych w nich zawartych (art. 6 ust. 1 pkt 2 i 3 ustawy o dostępie do informacji publicznej).

Szczegółowe standardy ujednoliconego systemu stron BIP obejmujące strukturę strony głównej Biuletynu, standardy struktury stron, na których udostępniają informacje publiczne organy władzy publicznej oraz inne podmioty wykonujące zadania publiczne, zakres i tryb przekazywania ministrowi właściwemu do spraw informatyzacji przez organy władzy publicznej oraz inne podmioty, informacji niezbędnych do zamieszczania na stronie głównej BIP, zostały określone w rozporządzeniu Ministra Spraw Wewnętrznych i Administracji z dnia 18 stycznia 2007 r. w sprawie Biuletynu Informacji Publicznej[140]. Czytelność informacji dla osób niepełnosprawnych w BIP uzyskuje się poprzez spełnienie wymagań zawartych w § 19 rozporządzenia KRI dotyczących zastosowania standardu WCAG 2.0.

[140] Dz. U. Nr 10, poz. 68.

Wykaz objętych kontrolą jednostek, osób zajmujących kierownicze stanowiska odpowiedzialnych za kontrolowaną działalność oraz ocen kontrolowanej działalności

Lp.	Nazwa jednostki objętej kontrolą	Osoby odpowiedzialne za kontrolowaną działalność		Ocena kontrolowanej działalności[141]
		Pełniona funkcja	Imię i nazwisko	
Jednostka organizacyjna NIK przeprowadzająca kontrolę – Departament Administracji Publicznej				
1.	Ministerstwo Administracji i Cyfryzacji	Minister	Rafał Trzaskowski (od 3 grudnia 2013 r.), wcześniej Michał Boni	O
2.	Urząd Miasta w Mińsku Mazowieckim	Burmistrz	Marcin Jakubowski	O
3.	Urząd Miasta Płocka	Prezydent Miasta	Andrzej Nowakowski	O
4.	Urząd Miejski w Pruszkowie	Prezydent Miasta	Jan Starzyński	O
5.	Urząd Miejski w Radomiu	Prezydent Miasta	Andrzej Kosztowniak	O
6.	Urząd Miejski w Zawierciu	Prezydent Miasta	Ryszard Mach do 17.07.2014 r. Od 18.07.2014 r. zadania i kompetencje Prezydenta Miasta przejął Pierwszy Zastępca Prezydenta Miasta Wojciech Mikuła	O
Jednostka organizacyjna NIK przeprowadzająca kontrolę – Delegatura NIK w Katowicach				
7.	Urząd Miejski w Dąbrowie Górniczej	Prezydent Miasta	Zbigniew Podraza	O
8.	Urząd Miasta Mikołów	Burmistrz	Marek Balcer	O
9.	Urząd Miejski w Mysłowicach	Prezydent Miasta	Edward Lasok	P
Jednostka organizacyjna NIK przeprowadzająca kontrolę – Delegatura NIK w Krakowie				
10.	Urząd Miejski w Andrychowie	Burmistrz	Tomasz Żak	O
11.	Urząd Miejski w Chrzanowie	Burmistrz	Ryszard Kosowski	O
12.	Urząd Miasta i Gminy w Olkuszu	Burmistrz	Dariusz Rzepka	O
13.	Urząd Miasta Nowy Targ	Burmistrz	Marek Fryźlewicz	O
Jednostka organizacyjna NIK przeprowadzająca kontrolę – Delegatura NIK w Poznaniu				
14.	Urząd Miasta Leszna	Prezydent Miasta	Tomasz Malepszy	O
15.	Urząd Miasta Luboń	Burmistrz	Dariusz Szmyt	O
16.	Urząd Miejski w Ostrowie Wielkopolskim	Prezydent Miasta	Jarosław Urbaniak	O
17.	Urząd Miejski w Śremie	Burmistrz	Adam Lewandowski	O
Jednostka organizacyjna NIK przeprowadzająca kontrolę – Delegatura NIK we Wrocławiu				
18.	Urząd Miasta Dzierżoniów	Burmistrz	Marek Piorun	O
19.	Urząd Miejski w Głogowie	Prezydent Miasta	Jan Kazimierz Zubowski	O
20.	Urząd Miasta Legnicy	Prezydent Miasta	Tadeusz Krzakowski	P
21.	Urząd Miejski w Świdnicy	Prezydent Miasta	Wojciech Murdzek	P
Jednostka organizacyjna NIK przeprowadzająca kontrolę – Delegatura NIK w Szczecinie				
22.	Urząd Miejski w Koszalinie	Prezydent Miasta	Piotr Jedliński	O
23.	Urząd Miejski w Stargardzie Szczecińskim	Prezydent Miasta	Sławomir Pajor	O
24.	Urząd Miasta w Szczecinku	Burmistrz	Jerzy Hardie-Douglas	O
25.	Urząd Miasta Świnoujście	Prezydent Miasta	Janusz Żmurkiewicz	O

[141] Użyty skrót oznacza: P – ocena pozytywna, O – ocena opisowa. NIK zastosowała w wystąpieniach pokontrolnych do kierowników kontrolowanych jednostek opisową formę oceny ogólnej kontrolowanej działalności wtedy, gdy działania lub stwierdzone nieprawidłowości w poszczególnych obszarach objętych kontrolą nie dawały podstaw do ogólnej oceny pozytywnej, jak również nie uzasadniały wydania ogólnej oceny negatywnej.

Wykaz najważniejszych aktów prawnych dotyczących kontrolowanej działalności

1. Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne[142].
2. Ustawa z dnia 6 września 2001 r. o dostępie do informacji publicznej[143].
3. Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych[144].
4. Rozporządzenie Prezesa Rady Ministrów z dnia 18 stycznia 2011 r. w sprawie instrukcji kancelaryjnej, jednolitych rzeczowych wykazów akt oraz instrukcji w sprawie organizacji i zakresu działania archiwów zakładowych[145].
5. Rozporządzenie Ministra Administracji i Cyfryzacji z 6 maja 2014 r. w sprawie zakresu i warunków korzystania z elektronicznej platformy usług administracji publicznej[146].
6. Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 27 kwietnia 2011 r. w sprawie zakresu i warunków korzystania z elektronicznej platformy usług administracji publicznej[147].
7. Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 18 stycznia 2007 r. w sprawie Biuletynu Informacji Publicznej[148].

[142] Dz. U. z 2014 r., poz. 1114.
[143] Dz. U. z 2014 r., poz. 782.
[144] Dz. U. z 2012 r., poz. 526 ze zm.
[145] Dz. U. Nr 14, poz. 67 ze zm.
[146] Dz. U. z 2014 r., poz. 584. Weszło w życie z dniem 11 maja 2014 r.
[147] Dz. U. Nr 93, poz. 546. Uchylone z dniem 11 maja 2014 r.
[148] Dz. U. Nr 10, poz. 68.

Wykaz organów, którym przekazano informację o wynikach kontroli

1. Prezydent Rzeczypospolitej Polskiej
2. Marszałek Sejmu Rzeczypospolitej Polskiej
3. Marszałek Senatu Rzeczypospolitej Polskiej
4. Prezes Rady Ministrów
5. Prezes Trybunału Konstytucyjnego
6. Rzecznik Praw Obywatelskich
7. Minister Administracji i Cyfryzacji
8. Przewodniczący Sejmowej Komisji Administracji i Cyfryzacji
9. Przewodniczący Sejmowej Komisji do Spraw Kontroli Państwowej
10. Przewodniczący Sejmowej Komisji Innowacyjności i Nowoczesnych Technologii
11. Przewodniczący Sejmowej Komisji Samorządu Terytorialnego i Polityki Regionalnej
12. Przewodniczący Sejmowej Komisji Ustawodawczej
13. Szef Kancelarii Prezydenta RP
14. Szef Kancelarii Prezesa Rady Ministrów
15. Szef Kancelarii Sejmu
16. Szef Kancelarii Senatu