NAJWYŻSZA IZBA KONTROLI
Delegatura w Poznaniu

LPO–4101-012-02/2014
P/14/004

WYSTĄPIENIE POKONTROLNE

NAJWYŻSZA IZBA KONTROLI
Delegatura w Poznaniu
ul. Dożynkowa 9H, 61-662 Poznań
T +48 61 655 62 00, F +48 61 655 62 01
lpo@nik.gov.pl

I. Dane identyfikacyjne kontroli

Numer i tytuł kontroli

P/14/004 – 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.

Jednostka przeprowadzająca kontrolę

Najwyższa Izba Kontroli
Delegatura w Poznaniu

Kontroler/Kontrolerzy]

1. Jacek Młynarczyk, główny specjalista kontroli państwowej, upoważnienie do kontroli nr 90973 z dnia 25 czerwca 2014 r.

(dowód: akta kontroli str. 1-2)

2. Wojciech Domagalski, główny specjalista kontroli państwowej, upoważnienie do kontroli nr 90974 z dnia 30 czerwca 2014 r.

(dowód: akta kontroli str. 44-45)

Jednostka kontrolowana

Urząd Miejski w Ostrowie Wielkopolskim

Kierownik jednostki kontrolowanej

Jarosław Urbaniak, Prezydent Miasta Ostrowa Wielkopolskiego.

(dowód: akta kontroli str. 3)

II. Ocena kontrolowanej działalności

Ocena ogólna

Prezydent Miasta Ostrowa Wielkopolskiego[1] w okresie od 31 maja 2012 r. do 25 lipca 2014 r., realizując zadania określone w rozporządzeniu 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[2] (dalej rozporządzenie w sprawie KRI):

- zapewnił współpracę zbadanych w toku kontroli systemów informatycznych z innymi systemami Urzędu, zgodnie z wymaganiami określonymi w § 5 ust. 3 pkt 3 rozporządzenia w sprawie KRI,

- inwentaryzował posiadany sprzęt informatyczny, zgodnie z § 20 ust. 2 pkt 2 rozporządzenia w sprawie KRI,

- zapewnił regularne tworzenie kopii zapasowych danych.

Ustalenia kontroli wykazały następującą nieprawidłowość przy realizacji zadań określonych w rozporządzeniu w sprawie KRI, tj. nie zrealizowano wymagań określonych w § 20 ust. 3 rozporządzenia w sprawie KRI, gdyż nie opracowano i nie

[1] Najwyższa Izba Kontroli stosuje 3-stopniową skalę ocen: pozytywna, pozytywna mimo stwierdzonych nieprawidłowości, negatywna. Jeżeli sformułowanie oceny ogólnej według proponowanej skali byłoby nadmiernie utrudnione, albo taka ocena nie dawałaby prawdziwego obrazu funkcjonowania kontrolowanej jednostki w zakresie objętym kontrolą, stosuje się ocenę opisową, bądź uzupełnia ocenę ogólną o dodatkowe objaśnienie.

[2] Dz. U. z 2012 r., poz. 526.

wdrożono Polityki Bezpieczeństwa Informacji (dalej PBI[3]), pomimo równoległego stosowania elektronicznego obiegu dokumentacji z zastosowaniem systemu informatycznego SKOK.

II. Opis ustalonego stanu faktycznego

1. Działania w zakresie dostosowania posiadanych systemów teleinformatycznych do współpracy z systemami/rejestrami używanymi przez inne podmioty administracji publicznej.

Opis stanu faktycznego

1.1. W dokumentacji strategicznej Ostrowa Wielkopolskiego uwzględniono działania dotyczące dostosowania Urzędu do elektronicznego świadczenia usług publicznych w terminie docelowym 2012 r., poprzez budowę: teleinformatycznej sieci wielokierunkowych połączeń; systemu wymiany informacji; internetowej platformy obsługi podmiotów gospodarczych i lokalnej społeczności przez samorząd terytorialny, instytucje oraz podmioty działające w obszarze użyteczności publicznej; systemu elektronicznej wymiany informacji dla obywatela w ramach inicjatywy e-Urząd oraz wspieranie inicjatyw budowania cyfrowych systemów wymiany wiedzy i nauczania /e-learning/. Prezydent Miasta decyzją nr 13/2014 z dnia 29 maja 2014 r. ustalił roczny plan pracy dla Urzędu z mocą obowiązującą od 1 stycznia 2014 r. W planie przewidziano: uruchomienie usług elektronicznych administracji w ramach „Budowy systemu informatycznego e-Ostrów Wielkopolski" na kwotę 84.000 zł; wdrożenie systemu publikacji elektronicznych planów zagospodarowania przestrzennego na kwotę 50.500 zł; wdrożenie systemu informatycznego przeznaczonego do zarządzania publicznym transportem zbiorowym (16.000 zł).

(dowód: akta kontroli str. 49-69, 89-95, 70-73, 97-99, 233-252)

1.2. Prezydent Miasta nie prowadził ankiet bądź innych form poznania potrzeb mieszkańców gminy dotyczących korzystania z elektronicznej formy komunikacji z urzędem, w konsekwencji nie było to przedmiotem ocen i analiz władz gminy.

(dowód: akta kontroli str. 70-72, 74-88, 178)

1.3. Po wejściu w życie rozporządzenia w sprawie KRI, Prezydent Miasta nie zwracał się do Ministra Administracji i Cyfryzacji z pytaniami lub prośbą o pomoc w zakresie dostosowania funkcjonujących w Urzędzie systemów/rejestrów informatycznych do wymogów KRI.

(dowód: akta kontroli str. 70-72, 74-88)

1.4. W myśl § 1 ust. 3 Instrukcji kancelaryjnej stanowiącej załącznik nr 1 do 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[4], Prezydent Miasta ustalił tradycyjny (papierowy) sposób dokumentowania przebiegu załatwiania i rozstrzygania spraw dla Urzędu. Z tych względów w Urzędzie brak było uregulowań określających zasady obiegu dokumentów w postaci elektronicznej. Sekretarz Miasta Ostrowa Wielkopolskiego upoważniony przez Prezydenta Miasta do składania wyjaśnień w toku

[3] Na niezbędność opracowania PBI wskazuje treść normy PN-ISO/IEC 27001:2007, do której odwołuje się § 20 ust. 3 rozporządzenia w sprawie KRI.

[4] Dz. U. z 2011 r. nr 14 poz. 67, ze zm.

kontroli w jego imieniu wyjaśnił, że najpóźniej do 30 czerwca 2015 r. zostanie uregulowany system elektronicznego obiegu dokumentacji. Prezydent Miasta podjął w toku kontroli NIK (11 lipca 2014 r.) działania w celu wprowadzenia regulacji wewnętrznej uwzględniającej zasady określone w KRI dotyczące interoperacyjności i stosowania modelu usługowego wdrażanych i modernizowanych systemów informatycznych Urzędu. Dokumentacja ta ma także określać formaty udostępnianych danych elektronicznych (zgodnie z załącznikiem nr 2 i 3 do rozporządzenia w sprawie KRI).

(dowód: akta kontroli str. 46-48, 50-73, 165-168, 212-214, 218-220, 223-231)

Na podstawie decyzji nr 4/2011 Prezydenta Miasta z dnia 31 stycznia 2011 r. czynności kancelaryjne wykonywane są w systemie tradycyjnym (w wersji papierowej), ale (równolegle) na każdym stanowisku pracy, stosowany był system komputerowej obsługi korespondencji „SKOK" o funkcjonalności systemu EZD[5]. System SKOK działał zgodnie z wymogami Instrukcji Kancelaryjnej i wykorzystywany był do: rejestrowania korespondencji przychodzącej, wewnętrznej i wychodzącej, (niezależnie) na stanowiskach pracy w każdej komórce organizacyjnej Urzędu, zapewnia rejestrację wszystkich pism (wpływających do Urzędu i sporządzanych w Urzędzie) w czasie rzeczywistym z zachowaniem jednolitej i spójnej chronologii numerów rejestrów w Urzędzie; dekretacji korespondencji przychodzącej w ramach hierarchii służbowej; prowadzenia rejestru spraw zgodnie z Jednolitym Rzeczowym Wykazem Akt; tworzenia i edycji w wersji elektronicznej dokumentów stanowiących korespondencję wewnętrzną i wychodzącą; raportowania o etapach załatwiania spraw na poszczególnych stanowiskach pracy; udostępniania przez internet klientom Urzędu informacji o etapie załatwiania ich spraw, poza przesyłaniem korespondencji w systemie SKOK urzędnicy pisali tradycyjnie pisma papierowe załatwiając sprawy wewnętrzne Urzędu, tj. procedowanie (rozpatrywanie) spraw odbywało się równolegle zarówno papierowo jak i elektronicznie. Prezydent Miasta planuje przejście z tradycyjnego obiegu korespondencji do obiegu elektronicznego w systemie EZD – jest to zadanie inwestycyjne, na realizację którego zabezpieczono środki finansowe w budżecie Miasta na 2014 r., w tym celu dokonano analizy obecnie używanego systemu obsługi korespondencji i rozpoznano rynek w zakresie dostępności innych systemów EZD – w Urzędzie zaprezentowano rozwiązania kilku dostawców oraz przeprowadzono testy wybranych systemów EZD.

(dowód: akta kontroli str. 70-72, 74-88, 147-152, 169)

1.5. W okresie od 31 maja 2012 r. do 31 maja 2014 r. złożono do Urzędu 93.262 dokumenty, w tym 93.240 (99,9%) w tradycyjnym papierowym systemie. Z Urzędu wyszło 43.390 dokumentów, w tym 43.368 (99,9%) w tradycyjnym papierowym systemie. Wniesione elektronicznie dokumenty dotyczyły udostępnienia informacji publicznej w 62 przypadkach (w tym 22 od obywateli, 38 od osób prawnych i firm oraz dwóch z innych urzędów) i innych spraw (zapytań) 27 przypadków (w tym z innego urzędu).

(dowód: akta kontroli str. 70-72, 74-88, 96)

1.6. Na dzień 30 maja 2012 r. Urząd nie świadczył usług elektronicznych. Pierwsze cztery usługi elektroniczne (złożenie deklaracji o wysokości opłaty za gospodarowanie odpadami komunalnymi; możliwość złożenia wniosku o przywrócenie terminu czynności procesowej; możliwość złożenia wniosku o wydanie zaświadczenia o figurowaniu (lub nie) w ewidencji podatników

[5] Elektroniczne Zarządzanie Dokumentacją,

podatku od nieruchomości, rolnego i leśnego; możliwość złożenia wniosku o udzielenie licencji oraz dokonanie zmiany licencji na wykonywanie transportu drogowego taksówką osobową) uruchomiono dopiero w toku kontroli (1 i 7 lipca 2014 r.) Opisy tych usług zawarte na stronach internetowych ePUAP[6] były aktualne i zgodne ze świadczonymi usługami.

(dowód: akta kontroli str. 100, 101)

1.7. Opisy procedur obowiązujących przy załatwianiu spraw z zakresu uruchomionych w toku kontroli usług świadczonych elektronicznie, po ich uruchomieniu, były publikowane w Biuletynie Informacji Publicznej. Opis zawierał dane dotyczące podmiotu realizującego usługę; miejsce świadczenia usługi, aktualnej podstawy prawnej i sposobu realizacji usługi.

(dowód: akta kontroli str. 100, 101-123)

1.8. Urząd nie przekazał wzorów dokumentów elektronicznych do centralnego repozytorium na ePUAP, gdyż korzystał ze wzorów dokumentów elektronicznych zamieszczonych na stronie ePUAP.

(dowód: akta kontroli str. 124)

1.9. Zakres współpracy[7] systemów informatycznych wewnątrz Urzędu zbadano w oparciu o trzy systemy i ustalono, że:

- system SKOK – posiada interoperacyjność na poziomie informacyjnym, pracownicy Urzędu wiedząc, że system SKOK gromadzi dane dotyczące rodzaju wpływającej, tworzonej i wychodzącej korespondencji oraz dane o sposobie i terminie załatwiania spraw, znajdują sposób dostępu do danych gromadzonych w tym systemie; system eksportuje dane do plików, które są wykorzystywane m.in. do zasilania innych systemów oraz do sporządzania okresowych zestawień dotyczących stanu załatwiania spraw oraz ilości korespondencji wpływającej i wychodzącej z podziałem na jej rodzaj i nadawcę,

- systemy PB_USC (Akty Stanu Cywilnego) i PB_EWID (Ewidencja Ludności) – posiadają interoperacyjność na poziomie jednostronnej komunikacji (komunikacja pomiędzy systemami odbywa się poprzez tabelę wymiany systemu PB_EWID), w celu przekazania danych o zmianie stanu cywilnego, urodzeniu lub zgonie osoby z systemu PB_USC należy wykonać eksport danych, a po stronie aplikacji PB_EWID otworzyć okno importu i zatwierdzić pobranie danych, import i eksport odbywają się poprzez uruchomienie przez użytkowników odpowiednich funkcji,

- system Odpady w gminie i system Taxi+ (system organu egzekucyjnego Prezydenta Miasta) posiadają interoperacyjność na poziomie jednostronnej komunikacji (proces wymiany informacji pomiędzy systemami odbywa się poprzez wyeksportowanie z systemu Odpady w gminie danych stanowiących

[6] Elektroniczna platforma usług administracji publicznej,

[7] Przyjęto możliwość wystąpienia jednego z pięciu poziomów współpracy: brak współpracy (interoperacyjności) wystąpi wówczas, gdy system nie komunikuje się z żadnym innym systemem IT, 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); 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; jednostronnej komunikacji, tj. dane z jednego systemu są przekazywane do innego systemu za pośrednictwem pracownika (operatora systemu), który dane te importuje ręcznie do systemu; 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; transakcyjny czyli wymiana danych pomiędzy systemami bez jakiegokolwiek pośrednictwa pracownika, czyli przekazywanie danych odbywa się w sposób w pełni zautomatyzowany.

treść tytułów wykonawczych oraz zaimportowanie tych danych do systemu Taxi+), import i eksport odbywają się poprzez uruchomienie przez użytkowników odpowiednich funkcji.

(dowód: akta kontroli str. 100, 101-125)

1.10. Interoperacyjność z innymi podmiotami administracji publicznej losowo wybranych pięciu (22,7%) spośród wszystkich 22 systemów informatycznych Urzędu: jeden - SKOK do poziomu informacyjnego[8] i cztery PB_USC (Akty Stanu Cywilnego) i PB_EWID (Ewidencja Ludności) oraz systemy „Odpady w Gminie" z „TAXI" (system organu egzekucyjnego Prezydenta Miasta) sprowadzała się do jednostronnej komunikacji[9]. Żaden z 22 systemów informatycznych Urzędu nie spełniał poziomu interoperacyjności w zakresie poziomu dwustronnej komunikacji[10] lub poziomu transakcyjnego[11].

(dowód: akta kontroli str. 125-129,173-177,125)

Powyższe systemy należy sklasyfikować jako działające na zasadzie informacyjnej lub jednostronnej komunikacji, tj. mające możliwość pobierania danych z innego systemu informatycznego z udziałem użytkowników systemu.

Stosownie do wymagań § 8 ust. 1 rozporządzenia w sprawie KRI, systemy służące do realizacji zadań publicznych zawierały rozwiązania oparte na modelu usługowym, bowiem można było zidentyfikować właściciela poszczególnych usług świadczonych przez Urząd, w opisie usługi był wskazany czas jej niedostępności, sposób zgłaszania awarii.

(dowód: akta kontroli str. 125-129,173-177,125)

W myśl § 23 rozporządzenia KRI systemy teleinformatyczne podmiotu realizującego zadania publiczne funkcjonujące przed wejściem w życie rozporządzenia KRI, należy dostosować do wymagań określonych w KRI nie później niż w dniu ich pierwszej istotnej modyfikacji przypadającej od 31 maja 2012 r. W okresie 2012-2014 (do zakończenia kontroli) Urząd zakupił nowe i dokonał istotnej modyfikacji (o co najmniej 10% wartości) dziewięciu posiadanych systemów informatycznych. Dopiero w toku kontroli Urząd podjął działania mające na celu świadczenie usług elektronicznych dla obywateli/klientów Urzędu i procedowania spraw w postaci elektronicznej. Dla osiągnięcia wyższego poziomu interoperacyjności zbudowano elektroniczną interakcję wewnątrz Urzędu (np. System ewidencji ludności „PB_EWID" <-> System USC „PB USC" i „Odpady w gminie" <-> TAXI+"), a także, jednostkowo w komunikacji z innymi urzędami administracji publicznej. Sekretarz Miasta wyjaśnił, że w przypadku sprawozdań budżetowych do RIO oraz Krajowego Biura Wyborczego uzyskano interoperacyjność na poziomie komunikacji jednostronnej.

(dowód: akta kontroli str. 50-73, 165-168)

1.11. Urząd nie zwracał się do innych jednostek administracji publicznej o prowadzenie wzajemnej komunikacji wyłącznie w formie elektronicznej.

---

[8] Pracownicy Urzędu posiadali jedynie wiedzę, że system ten gromadzi dane o wpływającej, tworzonej i wychodzącej korespondencji, umożliwiając sporządzanie okresowych zestawień w zakresie stanu załatwiania spraw oraz ilości korespondencji wpływającej i wychodzącej z podziałem na jej rodzaj i nadawcę.

[9] Dane z jednego systemu są przekazywane do innego systemu za pośrednictwem pracownika (operatora systemu), który dane te importuje ręcznie do systemu, poprzez uruchomienie odpowiednich funkcji.

[10] Dane z jednego systemu „A" przekazywane są do systemu „B", przy czym system „B" samodzielnie odnotowuje, że oczekują dane które mogą być zaimportowane.

[11] Wymiana danych pomiędzy systemami w sposób w pełni zautomatyzowany.

Interoperacyjność systemów informatycznych Urzędu ograniczała się do poziomu informacyjnego lub komunikacji jednostronnej z innymi jednostkami administracji publicznej[12]: W powyższym zakresie systemy informatyczne Urzędu z systemami innych urzędów administracji publicznej nie spełniały wymagań interoperacyjności osiąganej poprzez wymienność określoną w § 4 ust. 1 pkt 2 KRI.

(dowód: akta kontroli str. 89-95, 70-72, 97-99, 125-129)

Ustalone nieprawidłowości

W działalności kontrolowanej jednostki w przedstawionym wyżej zakresie nie stwierdzono nieprawidłowości.

Uwagi dotyczące badanej działalności

Zdaniem NIK, wprowadzenie systemu elektronicznego prowadzenia spraw, jako podstawowego systemu wykonywania czynności kancelaryjnych w Urzędzie, w miejsce aktualnie wykorzystywanego systemu tradycyjnego („papierowego") usprawni i przyśpieszy ich bieg. Podobnie korzystny efekt przyniesie dalsze dostosowywanie pozostałych systemów informatycznych Urzędu do wymagań interoperacyjności, o której mowa w § 5 ust. 3 pkt 3 KRI.

(dowód: akta kontroli str. 70-72, 89-95, 97-99, 125-129)

Ocena cząstkowa

W Urzędzie podjęto właściwe działania w zakresie: zapewnienia współpracy zbadanych systemów informatycznych, w tym uruchomienie w toku kontroli czterech usług elektronicznych, z innymi systemami informatycznymi Urzędu, choć dotychczas nie osiągnięto najwyższych poziomów ich interoperacyjności. Prawidłowe jest także, zadeklarowane przez Prezydenta Miasta, kontynuowanie działań w celu dostosowania pozostałych systemów informatycznych Urzędu do wymagań § 5 ust. 3 pkt 3 rozporządzenia KRI.

2. Wdrożenie systemu zarządzania bezpieczeństwem systemów informatycznych.

Opis stanu faktycznego

2.1. Prezydent Miasta, decyzją nr 9/2014 z dnia 26 marca 2014 r. w sprawie dokumentacji ochrony danych osobowych w Urzędzie Miejskim w Ostrowie Wielkopolskim, wprowadził w życie Dokumentację Ochrony Danych Osobowych w Urzędzie Miejskim w Ostrowie Wielkopolskim. W dokumentacji tej określono m.in.: najważniejsze zagadnienia ochrony danych osobowych, w tym: zagrożenia bezpieczeństwa; Politykę Bezpieczeństwa; instrukcję zarządzania systemem informatycznym. Regulacje te stosowane jednak były tylko w zakresie systemów przeznaczonych do przetwarzania danych osobowych. Prezydent Miasta przygotowuje regulacje określające zasady bezpieczeństwa pozostałych systemów informatycznych (nie zawierających danych osobowych). Dokumentacja ta ma uwzględniać wymagania określone w § 20 ust. 1 oraz § 20 ust. 2 pkt 1 KRI.

(dowód: akta kontroli str. 9-43, 70)

[12] Portal Informacyjny Administracji (PIA) wykorzystywany był m.in. do przesyłania z systemu Ewidencja Ludności paczek z danymi „PESEL" do Ministerstwa Spraw Wewnętrznych; system Besti@ - wykorzystywany był do elektronicznego przesyłania sprawozdań budżetowych do Regionalnej Izby Obrachunkowej; system CEiDG – wykorzystywany był do eksportu danych z bazy danych Urzędu; Edytor Aktów Prawnych – służył wysyłaniu elektronicznych wniosków o publikację aktów prawnych w Wielkopolskim Urzędzie Wojewódzkim; system Płatnik – wykorzystywany był do przesłania danych o osobach zatrudnionych w Urzędzie, na potrzeby rozliczeń z Urzędem Skarbowym. W Urzędzie przesyłano poprzez platformę ePUAP dane elektroniczne do Biura Obsługi Informatyki w Wielkopolskim Urzędzie Wojewódzkim.

2.2. Urząd posiadał zinwentaryzowany sprzęt informatyczny i podjął działania zapobiegające możliwości nieautoryzowanego instalowania oprogramowania (spełniając tym samym wymagania § 20 ust. 2 i ust. 4 KRI). W wyniku przeprowadzonych oględzin 10 komputerów stwierdzono, że ich użytkownicy nie posiadali uprawnień umożliwiających instalację nowego oprogramowania. Oprogramowanie w komputerach odpowiadało danym zawartym w oprogramowaniu inwentaryzacyjnym. Wyjątki stanowiły uaktualnienia oprogramowania oraz inne komponenty systemu operacyjnego lub narzędzia dodatkowe pozostałych aplikacji.

(dowód: akta kontroli str. 131-146, 153-157, 253-275)

2.3. Stosownie do wymagań § 20 ust. 2 pkt 3 KRI, w Urzędzie przeprowadzono dwie okresowe analizy ryzyka utraty integralności, poufności i dostępności informacji (24 marca 2014 r. oraz 30 czerwca 2014 r.). W wyniku przeprowadzonych analiz ustalono „małe ryzyko", w związku z tym stwierdzono brak konieczności wdrażania dodatkowych działań zmniejszających stopień ww. ryzyka.

(dowód: akta kontroli str.131-146)

2.4. Procedury nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemach informatycznych oraz wskazanie osoby odpowiedzialnej za te czynności zostały określone w Dokumentacji Ochrony Danych Osobowych w Urzędzie Miejskim. W przypadku tych systemów, o przyznaniu uprawnień decyduje Prezydent Miasta, natomiast w pozostałych przypadkach, kierownicy komórek organizacyjnych. Na podstawie tych decyzji, uprawnienia użytkownikom systemów informatycznych w Urzędzie nadawał Administrator Systemów Informatycznych, który także aktualizował uprawnienia. Administrator Bezpieczeństwa Informatycznego prowadził ewidencję w zakresie osób upoważnionych do przetwarzania danych osobowych. Ewidencja ta zawierała dane osoby upoważnionej, datę nadania i ustania oraz zakres upoważnienia, a także identyfikator dostępowy do tego programu. Zgodnie z § 20 ust. 2 pkt 4 rozporządzenia w sprawie KRI zarządzanie bezpieczeństwem informacji realizowane jest m.in. poprzez podejmowanie działań zapewniających, że osoby zaangażowane w proces przetwarzania informacji posiadają stosowne uprawnienia. Ustalono, że sporządzono procedury dotyczące zarządzania uprawnieniami użytkowników przetwarzających dane osobowe. W myśl § 20 ust. 3 rozporządzenia w sprawie KRI wymagania w zakresie zarządzania bezpieczeństwem informacji uznaje się za spełnione, jeżeli system zarządzania bezpieczeństwem informacji został opracowany na podstawie Polskiej Normy PN-ISO/IEC27001:2007. Zgodnie z normą PN-ISO/IEC27001:2007, załącznik A punkt A.11.2.1, zarządzanie uprawnieniami powinno być realizowane w oparciu o formalną procedurę rejestrowania i wyrejestrowywania użytkowników.

Kontrolerzy NIK dokonali przeglądu uprawnień do systemów i zasobów informatycznych Urzędu dla 18 pracowników, z którymi w kontrolowanym okresie rozwiązano stosunek pracy i nie stwierdzono, by nadal posiadały one dostęp do systemów informatycznych Urzędu.

(dowód: akta kontroli str.131-146,189,165-168)

2.5. W zakresie realizacji wymagań § 20 ust. 2 pkt 6 KRI ustalono, że w miesiącach lutym i marcu 2014 r. przeprowadzono cykl szkoleń z zakresu

ochrony danych osobowych oraz stosowania „Dokumentacji Ochrony Danych Osobowych w Urzędzie Miejskim w Ostrowie Wielkopolskim", która zawiera opis zasad bezpiecznego przetwarzania danych w systemie informatycznym Urzędu. Przeszkolono 99,51% pracowników Urzędu z zakresu zagrożenia bezpieczeństwa informacji, skutków naruszenia zasad bezpieczeństwa informacji, w tym odpowiedzialności prawnej wynikającej z ustawy o ochronie danych osobowych, sposobu stosowania środków koniecznych dla zapewnienia bezpieczeństwa informacji. Poza szkoleniem w ww. zakresie innych szkoleń odnośnie ochrony pozostałych informacji jakie są przetwarzane w Urzędzie (nie stanowiących danych osobowych), nie prowadzono.

(dowód: akta kontroli str.131-146, 216)

2.6. W Urzędzie, w kontrolowanym okresie pracownicy nie mieli możliwości mobilnego przetwarzania danych i pracy na odległość, w związku z powyższym Prezydent Miasta nie ustanowił zasad gwarantujących bezpieczną pracę przy przetwarzaniu mobilnym i pracy na odległość (§ 20 ust. 2 pkt 8 KRI). Prezydent Miasta ustanowił natomiast zasady regulujące korzystanie przez pracowników z komputerów przenośnych poza miejscem zatrudnienia.

(dowód: akta kontroli str.132, 158,159)

2.7. W zbadanych czterech umowach serwisowych, wykonawcy usługi serwisowej lub gwarancyjnej oraz napraw byli zobowiązani do zachowania w tajemnicy wszelkich informacji, w której posiadanie weszli w związku z realizacją umowy. Wykonawca był zobowiązany zachować w tajemnicy dane uzyskane z systemów komputerowych Urzędu zarówno w czasie trwania umowy, jak również po jej wygaśnięciu oraz do nieudostępniania ich osobom trzecim.

(dowód: akta kontroli str.160-164,186-210)

W Urzędzie obowiązywała procedura zgłaszania zdarzeń powodujących naruszenie bezpieczeństwa ochrony danych osobowych opisana w Dokumentacji ochrony danych osobowych w urzędzie. Wzór raportu z naruszenia bezpieczeństwa zasad ochrony danych osobowych określono w załączniku do tej dokumentacji. Podczas szkoleń (w miesiącach luty i marzec 2014 r.) dotyczących stosowania tej dokumentacji, pracownicy Urzędu zostali zapoznani z tą procedurą, w związku z powyższym, każde naruszenie zasad bezpieczeństwa danych osobowych podlegało zgłoszeniu. W kontrolowanym okresie nie odnotowano takich zgłoszeń.

(dowód: akta kontroli str. 9-43,131-132)

W Urzędzie były regularnie tworzone kopie zapasowe baz danych systemów informatycznych oraz oprogramowania aplikacyjnego. Kopie zapasowe tworzone były zgodnie z Dokumentacją Ochrony Danych Osobowych w Urzędzie Miejskim w Ostrowie Wielkopolskim. Kopie zapasowe przechowywane były prawidłowo, w siedzibie Urzędu na zewnętrznych dyskach twardych oraz na dyskach macierzy. Dane wyjściowe z systemów informatycznych Urzędu udostępniane były m.in. w formatach (doc. Xls. XML Otago, XML Technika) ujętych na liście formatów danych zapewniających dostęp do zasobów informacji opublikowanej w załączniku nr 2 do rozporządzenia w sprawie KRI.

(dowód: akta kontroli str.105, 110, 115, 120, 125, 126,131-132, 9-43, 171-174)

W kontrolowanym okresie, poza ochroną danych osobowych nie prowadzono audytu bezpieczeństwa informacji. Audyt taki, według informacji Prezydenta Miasta będzie przeprowadzony w 2014 r., a kopie zapasowe były tworzone zgodnie z Dokumentacją Ochrony Danych.

(dowód: akta kontroli str.170-173)

Ustalone nieprawidłowości

W działalności kontrolowanej jednostki, w przedstawionym wyżej zakresie, stwierdzono następującą nieprawidłowość:

Ustalono, że w Urzędzie nie opracowano i nie wdrożono PBI, która jest elementem systemu zarządzania bezpieczeństwem informacji. Zauważyć należy, że w Urzędzie obok tradycyjnego systemu załatwiania spraw, pomocniczo funkcjonował elektroniczny system obiegu dokumentacji. Mając na uwadze powyższe, trzeba wskazać, że w myśl § 20 ust. 3 rozporządzenia w sprawie KRI, wymagania w zakresie systemu zarządzania bezpieczeństwem informacji uznaje się za spełnione jeżeli zostały opracowane na podstawie Polskich Norm PN-ISO/IEC27001:2007 Technika informatyczna, Techniki bezpieczeństwa. Systemy zarządzania bezpieczeństwem informacji oraz PN-ISO/IEC 17799:2007 Technika informatyczna. Techniki bezpieczeństwa. Praktyczne zasady zarządzania bezpieczeństwem informacji. W punkcie 5.1.1. normy PN-ISO/IEC17799 wskazuje się, aby opracowano i stosowano w Urzędzie dokument polityki bezpieczeństwa informacji. Prace związane z przygotowaniem i wprowadzeniem tego dokumentu rozpoczęto już w toku kontroli NIK.

(dowód: akta kontroli str.70-73, 165-169)

Ocena cząstkowa

W ocenie NIK, Prezydent Miasta częściowo wywiązał się z realizacji przepisów rozporządzenia w sprawie KRI. Właściwie zinwentaryzowano posiadany sprzęt oraz zablokowano możliwości swobodnego instalowania oprogramowania w posiadanych systemach informatycznych. Prawidłowo skonstruowano w zawieranych umowach serwisowych postanowienia mające zagwarantować odpowiedni poziom bezpieczeństwa informacji. Nie została natomiast opracowana PBI.

3. Zapewnienie dostępności informacji Urzędu dla osób niepełnosprawnych.

Opis stanu faktycznego

3.1. Strona BIP Urzędu nie zawierała udogodnień dla potrzeb osób niepełnosprawnych. W wyniku weryfikacji stron internetowych kontrolowanej jednostki www.ostrow-wielkopolski.um.gov.pl oraz www.bip.ostrow-wielkopolski.um.gov.pl ze standardem WCAG 2.0, który służy dostosowaniu wyświetlanej treści na stronie internetowej do potrzeb osób niedowidzących, przeprowadzonej za pomocą narzędzi dostępnych na stronach http://validator.w3.org oraz http://jigsaw.w3.org/css-validator stwierdzono błędy i ostrzeżenia. Strona internetowa Urzędu o adresie www.ostrow-wielkopolski.um.gov.pl posiadała ułatwienie korzystania z niej przez osoby z niepełnosprawnością wzroku, polegające na możliwości odsłuchania treści zamieszczonej wiadomości poprzez jej odczytanie przez stronę internetową. Prezydent Miasta podał, że dla właściwej dostępności informacji Urzędu dla osób niepełnosprawnych dokonał wyboru wykonawcy audytu dostępności strony internetowej Urzędu, w zakresie spełnienia przez ww. stronę normy WCAG 2.0. Zlecenie przeprowadzenia audytu zaplanował w miesiącu lipcu 2014 r. Na podstawie wyników audytu, przed 30 maja 2015 r., zlecona

zostanie modyfikacja strony w celu zapewnienie jej pełnej zgodności z normą WCAG 2.0. Strona internetowa Urzędu, według oświadczenia kierownika Referatu Informatyki i Telekomunikacji, zostanie sprawdzona pod względem dostosowania jej do pozostałych wymagań § 19 KRI w terminie do 5 sierpnia 2014 r.

(dowód: akta kontroli str.71-72)

Ustalone nieprawidłowości

W działalności kontrolowanej jednostki w przedstawionym wyżej zakresie nie stwierdzono nieprawidłowości.

IV. Wniosek

Wnioski pokontrolne

Przedstawiając powyższe oceny i uwagi wynikające z ustaleń kontroli, Najwyższa Izba Kontroli, na podstawie art. 53 ust. 1 pkt 5 ustawy z dnia 23 grudnia 1994 r. o Najwyższej Izbie Kontroli[13], wnosi o: kontynuację podjętych działań na rzecz wdrożenia Polityki Bezpieczeństwa Informacji określającej zasady bezpieczeństwa informacji w Urzędzie.

V. Pozostałe informacje i pouczenia

Prawo zgłoszenia zastrzeżeń

Wystąpienie pokontrolne zostało sporządzone w dwóch egzemplarzach; jeden dla kierownika jednostki kontrolowanej, drugi do akt kontroli.

Zgodnie z art. 54 ustawy o NIK kierownikowi jednostki kontrolowanej przysługuje prawo zgłoszenia na piśmie umotywowanych zastrzeżeń do wystąpienia pokontrolnego, w terminie 21 dni od dnia jego przekazania. Zastrzeżenia zgłasza się do dyrektora Delegatury NIK w Poznaniu.

Obowiązek poinformowania NIK o sposobie wykorzystania uwag i wykonania wniosków

Zgodnie z art. 62 ustawy o NIK, proszę o poinformowanie Najwyższej Izby Kontroli, w terminie 21 dni od otrzymania wystąpienia pokontrolnego, o sposobie wykorzystania uwag i wykonania wniosku pokontrolnego oraz o podjętych działaniach lub przyczynach niepodjęcia tych działań.

[13] Dz. U. z 2012 r., poz. 82, ze zm.

W przypadku wniesienia zastrzeżeń do wystąpienia pokontrolnego, termin przedstawienia informacji liczy się od dnia otrzymania uchwały o oddaleniu zastrzeżeń w całości lub zmienionego wystąpienia pokontrolnego.

Poznań, dnia **7** sierpnia 2014 r.

Najwyższa Izba Kontroli
Delegatura w Poznaniu

Kontroler
Jacek Młynarczyk
Główny specjalista kontroli państwowej

.....
Podpis

Dyrektor
z up. Tomasz Nowiński
Wicedyrektor

.....
Podpis

Kontroler
Wojciech Domagalski
Główny specjalista kontroli państwowej

.....
Podpis