NAJWYŻSZA IZBA KONTROLI
Delegatura we Wrocławiu

LWR-4101-013-04/2014
P/14/004

WYSTĄPIENIE POKONTROLNE

NAJWYŻSZA IZBA KONTROLI
Delegatura we Wrocławiu
ul. Marszałka J. Piłsudskiego 15/17, 50-044 Wrocław
T +48 71 711 83 00, F +48 71 711 83 50
lwr@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.

Jednostka przeprowadzająca kontrolę

Najwyższa Izba Kontroli, Delegatura we Wrocławiu

Kontroler

Mariusz Orawczak – starszy inspektor kontroli państwowej, upoważnienie do kontroli nr 89789 z dnia 17 czerwca 2014 r.

(dowód: akta kontroli str. 1-2)

Jednostka kontrolowana

Urząd Miejski w Świdnicy (dalej: Urząd).

Kierownik jednostki kontrolowanej

Wojciech Murdzek – Prezydent Świdnicy (dalej: Prezydent).

(dowód: akta kontroli str. 3)

II. Ocena kontrolowanej działalności

Ocena ogólna

Najwyższa Izba Kontroli ocenia pozytywnie[1] działania Prezydenta Świdnicy, w zakresie wdrożenia wybranych wymagań nałożonych na systemy informatyczne przez rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. *w sprawie Krajowych Ram Interoperacyjności oraz minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych*[2] (dalej: *rozporządzenie KRI*) w okresie od 31 maja 2012 r. do 20 sierpnia 2014 r.

Uzasadnienie oceny ogólnej

Powyższą ocenę ogólną uzasadniają ustalenia kontroli dotyczące w szczególności: [1] korzystania z elektronicznego obiegu dokumentów wewnątrz Urzędu; [2] udostępnienia klientom Urzędu 19 usług elektronicznych za pośrednictwem Elektronicznej Platformy Usług Administracji Publicznej ePUAP, [3] wspierania w podstawowym zakresie modelu usługowego w procesie zarządzania usługami elektronicznymi Urzędu, [4] zapewnienia współpracy pomiędzy wybranymi do kontroli systemami informatycznymi w sposób spełniający minimalne wymogi w zakresie interoperacyjności, [5] opracowania i wdrożenia do stosowania Polityki Bezpieczeństwa Informacji, [6] zablokowania możliwości swobodnego instalowania oprogramowania w posiadanych systemach informatycznych, [7] zawierania w umowach serwisu oprogramowania oraz zakupu komputerów postanowień gwarantujących odpowiedni poziom bezpieczeństwa informacji, [8] zapewnienia audytu wewnętrznego w zakresie bezpieczeństwa informacji, [9] właściwego sposobu przechowywania i zabezpieczenia kopii zapasowych danych.

III. Opis ustalonego stanu faktycznego

1. Działania w zakresie dostosowania posiadanych systemów teleinformatycznych do współpracy z innymi systemami/rejestrami informatycznymi

[1] Najwyższa Izba Kontroli stosuje 3-stopniową skalę ocen: pozytywna, pozytywna mimo stwierdzonych nieprawidłowości, negatywna.

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

Opis stanu faktycznego

1.1. Strategia Miasta Świdnicy – *Świdnica w perspektywie pokoleniowej*, przyjęta uchwałą[3] Rady Miejskiej w Świdnicy uwzględnia w swojej treści konieczność wykorzystywania nowoczesnych technologii w komunikacji pomiędzy mieszkańcami Świdnicy oraz władzami Miasta, reprezentującymi zarówno Urząd Miejski w Świdnicy jak i jednostki organizacyjne Gminy Miasta Świdnica. Jednym z założeń strategii było wykorzystywanie przez władze Miasta nowoczesnych technologii do komunikacji oraz rozbudowy platformy stałej wymiany poglądów między władzą samorządową i mieszkańcami.

(dowód: akta kontroli str. 6, 14-18, 19-23)

1.2. Urząd nie dokonał analizy potrzeb w zakresie działań promocyjnych ukierunkowanych na komunikację elektroniczną. Prezydent wyjaśnił, że Urząd Miejski w Świdnicy przy okazji podejmowanych działań, akcji, czy też różnych przedsięwzięć promował rozwiązania komunikacji elektronicznej. Decyzja taka wynikała z postrzegania funkcjonowania świdnickiej administracji, jako nowoczesnego i sprawnego urzędu, gdzie mieszkańcy i przedsiębiorcy mają nie tylko dostęp do usług wysokiej jakości, ale też do łatwego kontaktu drogą elektroniczną. Grupą docelową działań mających na celu promowanie komunikacji elektronicznej byli wszyscy mieszkańcy, którzy korzystali z dostępu do Internetu niezależnie od wieku.

(dowód: akta kontroli str. 6-8)

1.3. W okresie objętym kontrolą nie badano potrzeb mieszkańców Świdnicy dotyczących potrzeb korzystania z usług elektronicznych oraz elektronicznej formy komunikacji z Urzędem.

(dowód: akta kontroli str. 8)

1.4. Urząd nie zwracał się do Ministra Administracji i Cyfryzacji z problemami, jak również z prośbą o pomoc w zakresie dostosowania systemów/rejestrów informatycznych do wymogów *rozporządzenia KRI*.

(dowód: akta kontroli str. 8)

1.5. W Urzędzie, w celu zarządzania obiegiem dokumentów i dokumentacją stosowane były procedury i zasady postępowania z dokumentami wpływającymi do Urzędu zawarte w Instrukcji Kancelaryjnej stanowiącej załącznik 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], co znalazło odzwierciedlenie w Regulaminie organizacyjnym Urzędu[5]. Przyjęto, stosownie do § 1 pkt 3 Instrukcji Kancelaryjnej, tradycyjny (papierowy) system wykonywania czynności kancelaryjnych, jako podstawowy sposób dokumentowania przebiegu załatwiania i rozstrzygania spraw w Urzędzie[6].

(dowód: akta kontroli str. 24-36, 318-320)

W Urzędzie wdrożono system zarządzania jakością według wymagań normy PN-EN ISO 9001:2001, którego certyfikacja wygasła w dniu 24 czerwca 2013 r. i funkcjonuje w oparciu o kontynuację „dobrych praktyk" wypracowanych w ramach tego certyfikatu. Opracowana Księga Jakości określiła system przyjmowania i postępowania z dokumentami dostarczonymi do Urzędu przez klienta, zgodnie z Instrukcją

---

[3] Uchwała nr XLII/500/2010 Rady Miejskiej w Świdnicy z dnia 19 lutego 2010 r.

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

[5] Zarządzenie nr 80/07 Prezydenta Miasta Świdnicy z dnia 14 marca 2007 r. w sprawie nadania Regulaminu Organizacyjnego Urzędu Miejskiego w Świdnicy, zmienione zarządzeniem nr 120-7/2011 Prezydenta Miasta Świdnicy z dnia 1 marca 2011 r.

[6] Zarządzenie nr 120-15/2011 Prezydenta Miasta Świdnicy z dnia 1 kwietnia 2011 r. w sprawie wyboru systemu wykonywania czynności kancelaryjnych w Urzędzie Miejskim w Świdnicy.

Kancelaryjną, w której przy załatwianiu spraw pracowników Urzędu obowiązuje forma pisemna papierowa.

(dowód: akta kontroli str. 318, 326-343)

Procedura obiegu dokumentów elektronicznych w Urzędzie była realizowana w oparciu o system zarządzania obiegiem dokumentów na platformie oprogramowania narzędziowego OfficeObjects®, wdrożonym w 2002 r. na podstawie postanowienia Zarządu Miasta Świdnicy[7].

(dowód: akta kontroli str. 8-9, 268-316, 321-325)

Praktyka stosowana w Urzędzie wykazuje system mieszany wykonywania czynności kancelaryjnych. Cała korespondencja przychodząca do Urzędu trafia do punktu Obsługi Interesantów, gdzie zostaje zarejestrowana w systemie elektronicznego obiegu dokumentów. Po zarejestrowaniu dokumenty papierowe są skanowane i w wersji cyfrowej dołącza się je do przedmiotowych spraw w systemie elektronicznego obiegu dokumentów. Ze względu na ograniczenia czasowe (mała obsada kadrowa – tylko dwie osoby przyjmujące korespondencję) nie skanuje się obszernych załączników do pism lub dokumentów dużych rozmiarów oraz przesyłek wpływających do Urzędu, które na mocy zarządzenia Prezydenta[8] nie są otwierane przez punkt kancelaryjny. Sporadycznie, w porozumieniu z innymi komórkami organizacyjnymi Urzędu, np. Urzędem Stanu Cywilnego, odstępuje się od skanowania pism. Po zeskanowaniu oryginalne dokumenty, równolegle do wersji elektronicznej, przekazywane są dalej do odpowiedniej komórki organizacyjnej w Urzędzie, zgodnie z dekretacją sprawy, której dotyczą. Dekretacji dokonuje pracownik punktu Obsługi Interesantów w systemie elektronicznego obiegu dokumentów, do odpowiedniej komórki organizacyjnej Urzędu (referatu) lub dyrektora odpowiedniego departamentu.

(dowód: akta kontroli str. 344-348)

1.6. W okresie od 31 maja 2012 r. do 31 maja 2014 r. do Urzędu wpłynęło 102 141 dokumentów, w tym 10 w formie elektronicznej, tj. 0,01%. W tym samym okresie z Urzędu wyszło 155 697 dokumentów, przy czym formę elektroniczną zastosowano wyłącznie w odniesieniu do 27 przypadków (0,02%).

(dowód: akta kontroli str. 13)

1.7. Do dnia 31 maja 2012 r. Urząd nie świadczył usług elektronicznych natomiast aktualnie świadczy 19 usług elektronicznych za pośrednictwem Elektronicznej Platformy Usług Administracji Publicznej ePUAP. Szczegółowym badaniem w zakresie zgodności świadczonej usługi z jej opisem zamieszczonym na stronie internetowej objęto pięć usług elektronicznych[9] świadczonych przez Urząd. Kontrola wykazała, że opisy wszystkich objętych badaniem usług były aktualne i zgodne z faktycznie świadczonymi.

(dowód: akta kontroli str. 108-111, 120-122)

1.8. Na stronie internetowej Urzędu umieszczono informację odnośnie obowiązujących procedur w zakresie załatwiania spraw drogą elektroniczną. Każda z badanych pięciu usług elektronicznych zawierała w karcie opisu usługi aktualne

---

[7] Zarządzenie nr 11/2002 Prezydenta Miasta Świdnicy z dnia 10 kwietnia 2002 r. w sprawie powołania zespołu do wdrożenia Systemu Komputerowej Obsługi Spraw, Dokumentów i Korespondencji, zgodnie z postanowieniem Zarządu Miasta Świdnicy z dnia 28 stycznia 2002 r.

[8] Zarządzenie nr 120-17/2011 Prezydenta Miasta Świdnicy z dnia 1 kwietnia 2011 r. w sprawie ustalenia „Listy rodzajów przesyłek wpływających do Urzędu Miejskiego w Świdnicy, które nie są otwierane przez punkt kancelaryjny".

[9] 1) Decyzja o uwarunkowaniach środowiskowych, 2) Odpisy i zaświadczenia z ksiąg stanu cywilnego, 3) Skargi, wnioski, zapytania do urzędu, 4) Uzgodnienie przebiegu projektowanej sieci lub przyłącza, 5) Wypisy i wyrysy z miejscowego planu zagospodarowania przestrzennego.

dane dotyczące podmiotu, miejsce świadczenia usługi, podstawę prawną, sposób realizacji usługi.

(dowód: akta kontroli str. 108, 112-119)

1.9. 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. 108)

1.10. Ustalono, że w procesie zarządzania usługami elektronicznymi Urząd w podstawowym zakresie wspiera model usługowy, zgodnie z definicją zawartą w § 2 pkt 8 *rozporządzenia KRI*. Zarządzanie usługami elektronicznymi realizowanymi przez Urząd odbywa się w oparciu o udokumentowane w systemie elektronicznego obiegu dokumentów procedury. Istnieją karty opisu usługi a ich aktualizacja następuje w miarę potrzeb i jest realizowana w obrębie komórki organizacyjnej Urzędu, realizującej konkretne usługi. Możliwe jest zidentyfikowanie właściciela poszczególnych usług na poziomie konkretnej komórki organizacyjnej Urzędu realizującej usługi. Nie określono jednak sposobu zgłaszania awarii, osób/komórek/podmiotów odpowiedzialnych za usuwanie awarii, technicznych właścicieli usług.

(dowód: akta kontroli str. 108-120, 151-152)

1.11. Zakres współpracy systemów informatycznych wewnątrz Urzędu zbadano w oparciu o dobór celowy czterech systemów, zakupionych po 31 maja 2012 r.[10], tj.:

1) Systemu Usług Publicznych – tworzy dedykowane katalogi usług publicznych na platformie ePUAP. System komunikuje się w sposób automatyczny, poprzez Elektroniczną Platformę Usług Administracji Publicznej ePUAP, z systemem elektronicznego obiegu dokumentów w Urzędzie;
2) Systemu „Książka Drogi" z podsystemem „obiekty mostowe" – nakładka na program Bentley Mapy (zaawansowanego systemu GIS do prowadzenia wszelkiego typu opracowań mapowych i projektów inżynierskich związanych z szeroko rozumianą infrastrukturą), która umożliwia oznaczanie i ewidencję dróg i obiektów mostowych. System pobiera mapy stworzone w programie Bentley Map. Dokonać tego musi obsługujący pracownik. Stworzone mapy z oznaczeniami drogowymi zapisywane są lokalnie na komputerze w celu dalszego wykorzystania, drukowania, udostępniania itp;
3) Systemu Gospodarowania Odpadami Komunalnymi GOK+ firmy RADIX – służy do gromadzenia informacji niezbędnych do prawidłowego funkcjonowania w Urzędzie ewidencji związanej z gospodarowaniem odpadami komunalnymi. System pobiera dane osobowe z Systemu Ewidencji Ludności ELUD+ oraz dane ewidencyjne z Systemu Naliczania Podatków od Gruntów i Nieruchomości POGRUN+. Pracownik musi wskazać dane, które mają być zaimportowane (np. przez wskazanie numeru PESEL) oraz musi udzielić zgodę na ich wczytanie. Możliwe jest wpisanie przez pracownika nowego obiektu, którego dane zostaną po jego akceptacji, wysłane do ELUD+ lub/i POGRUN+. System GOK+, po zatwierdzeniu przez pracownika, eksportuje dane z należnościami do Systemu Windykacji Opłat i Podatków WIP+;
4) Systemu Windykacji Opłat i Podatków WIP+ firmy RADIX. System pobiera dane osobowe z Systemu Ewidencji Ludności ELUD+ oraz Systemu Informacji o Mieszkańcach, Właścicielach i Użytkownikach INFO+. Pracownik musi wskazać dane, które mają być zaimportowane (np. przez wskazanie numeru PESEL) oraz musi udzielić zgodę na ich wczytanie. Możliwe jest wpisanie przez pracownika nowego obiektu, którego dane zostaną po jego akceptacji, wysłane do ELUD+ lub/i

[10] Data wejścia w życie *rozporządzenia KRI*.

INFO+. System WIP+, po zatwierdzeniu przez pracownika, importuje dane z należnościami z innych systemów firmy RADIX zainstalowanych w Urzędzie, w tym z Systemu Gospodarowania Odpadami Komunalnymi GOK+. System WIP+, po zatwierdzeniu przez pracownika, komunikuje się dwustronnie także z Systemem Obsługi Kasy KASA+, Systemem Finansowo-Księgowym Księgowości Budżetowej FKB+, Systemem Naliczania Podatków od Gruntów i Nieruchomości POGRUN+.

Poziom współpracy (interoperacyjności) tych systemów można sklasyfikować, jako:

- jednostronnej komunikacji[11] - systemu „Książka Drogi" z podsystemem „obiekty mostowe";
- dwustronnej komunikacji[12] - System Gospodarowania Odpadami Komunalnymi GOK+, System Windykacji Opłat i Podatków WIP+;
- transakcyjny[13] - System Usług Publicznych.

W ocenie NIK badane systemy informatyczne spełniają minimalne wymogi interoperacyjności w zakresie współpracy z innymi systemami Urzędu określone w § 5 ust.3 pkt 3 *rozporządzenia KRI*.

(dowód: akta kontroli str. 252-267)

1.12. Elektroniczna komunikacja z innymi jednostkami administracji publicznej w zakresie funkcjonowania i realizacji poszczególnych zadań Urzędu funkcjonuje głównie w oparciu o określone regulacje prawne. Urząd nie zwracał się do innej jednostki administracji publicznej z wnioskiem o prowadzenie wzajemnej komunikacji wyłącznie w formie elektronicznej. Również inny organ administracji publicznej nie zwrócił się z wnioskiem do Urzędu o prowadzenie wzajemnej komunikacji wyłącznie w formie elektronicznej.

(dowód: akta kontroli str. 9-10, 152)

Wyjaśniając, jaki zakres danych jest wymieniany pomiędzy systemami Urzędu a innymi systemami w administracji publicznej Prezydent podał, że:

- pomiędzy systemami wykorzystywanymi w Departamencie Budżetowo-Finansowym, a innymi systemami w administracji publicznej (RIO, DUW, KBW) przekazywane były dane objęte systemem sprawozdawczości budżetowej, sprawozdawczości statystycznej (GUS), systemem rozliczeń ZUS, PFRON;
- przekazywanie sprawozdań budżetowych przez jednostki budżetowe realizowane było wyłącznie w formie elektronicznej (dane objęte systemem sprawozdawczości budżetowej);
- SHRIMP - dane o udzielonej pomocy publicznej (tj. podstawa prawna, dzień udzielenia pomocy publicznej, jej wielkość, nazwa beneficjenta, NIP, PKD, wartość pomocy publicznej, z jakich środków);
- Legislator - treść uchwały w formacie XML;
- Centralna Ewidencja Informacji o Działalności Gospodarczej (CEIDG) - dane zawarte we wniosku CEIDG-1;
- SIIS - zakres danych określony rozporządzeniem Ministra Administracji i Cyfryzacji z dnia 24 lutego 2014 r. *w sprawie inwentaryzacji infrastruktury i usług telekomunikacyjnych*;
- WebEWID - dane przestrzenne i dane z zakresu ewidencji gruntów;

---

[11] Dane z jednego systemu są przekazywane do innego systemu za pośrednictwem pracownika (operatora systemu), który dane te importuje ręcznie do systemu.

[12] 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.

[13] Wymiana danych pomiędzy systemami bez jakiegokolwiek pośrednictwa pracownika, czyli przekazywanie danych odbywa się w sposób w pełni zautomatyzowany.

- SESPID - w ramach systemu wymieniane były dane z ewidencji ludności, ewidencji działalności gospodarczej, systemu dodatków mieszkaniowych. Z innych urzędów otrzymywano dane z systemu opieki społecznej z MOPS Świdnica, ewidencji bezrobotnych Powiatu Świdnickiego, systemu ewidencji Powiatowego Centrum Pomocy Rodzinie;
- APUSC - oprogramowanie służące do rejestracji i przekazywania danych statystycznych z zakresu rejestracji urodzeń, małżeństw i zgonów. APUSC służy do tworzenia dokumentów elektronicznych, zgodnych z opublikowaną przez GUS specyfikacją oraz ich wysyłanie za pośrednictwem Internetu na serwer GUS bezpiecznym kanałem komunikacyjnym w oparciu o protokół SSL z szyfrowaniem przekazywanych danych;
- Platforma wyborcza – umożliwiała elektronicznie określać obwodowe komisje wyborcze, kandydatów do wyborów oraz dokonywać czynności technicznych umożliwiających przygotowanie protokołów z wynikami głosowania w obwodach w noc wyborczą;
- Portal Informacyjny Administracji MSW (PIA) - pomiędzy systemami wymieniane są dane, które Urząd przetwarzał z zakresu ewidencji ludności i dowodów osobistych oraz rejestru wyborców.

(dowód: akta kontroli str. 10-11)

Żaden z czterech systemów poddanych badaniu nie komunikował się z systemem IT innych jednostek administracji publicznej.

(dowód: akta kontroli str. 252, 263-265)

Ustalone nieprawidłowości

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

Uwagi dotyczące badanej działalności

1. NIK zauważa, iż formalne 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, zwłaszcza, że brak jest ku temu przeszkód technicznych (obieg dokumentów elektronicznych w Urzędzie jest realizowany w oparciu o profesjonalny system informatyczny od 12 lat). Przyczyni się to do wyeliminowania mieszanego, dublującego się systemu wykonywania czynności kancelaryjnych, prowadzonych obecnie zarówno w formie papierowej jak i elektronicznej.
2. Zarządzanie usługami elektronicznymi realizowanymi przez Urząd odbywa się w oparciu o udokumentowane karty opisu usług oraz procedury elektronicznego obiegu dokumentów w Urzędzie. W ocenie NIK, zapewnienie sprawnego świadczenia usług elektronicznych wymaga jednak podjęcia dalszych działań dla jego usprawnienia. W tym celu konieczne jest opracowanie odrębnych wymagań dla każdej ze świadczonych usług elektronicznych zawierających, co najmniej imiennie wskazanie jej właściciela, dopuszczalnych okresów niedostępności usługi, określenie zakładanego rozłożonego w czasie zapotrzebowania klientów Urzędu na usługę (obciążenie).

Ocena cząstkowa

Najwyższa Izba Kontroli ocenia pozytywnie działalność kontrolowanej jednostki w zakresie dostosowania posiadanych systemów teleinformatycznych do współpracy z systemami/rejestrami używanymi przez inne podmioty administracji publicznej.
Powyższą ocenę cząstkową uzasadniają ustalenia kontroli dotyczące w szczególności: [1] korzystania z elektronicznego obiegu dokumentów wewnątrz Urzędu; [2] udostępnienia klientom Urzędu 19 usług elektronicznych za pośrednictwem Elektronicznej Platformy Usług Administracji Publicznej ePUAP; [3] wspierania w podstawowym zakresie modelu usługowego w procesie zarządzania usługami elektronicznymi Urzędu; [4] zapewnienia współpracy pomiędzy wybranymi

do kontroli systemami informatycznymi w sposób spełniający minimalne wymogi w zakresie interoperacyjności.

2. Wdrożenie systemu zarządzania bezpieczeństwem systemów informatycznych

Opis stanu faktycznego

2.1. Urząd posiadał opracowaną i wdrożoną do stosowania Politykę Bezpieczeństwa Informacji (dalej PBI), zgodną z normą PN-ISO/IEC 27001:2007[14] oraz Instrukcję zarzadzania systemami informatycznymi. Dokumenty te zostały zatwierdzone przez Prezydenta[15] oraz przedstawione do zapoznania się i stosowania wszystkim pracownikom zgodnie z § 20 ust. 1 *rozporządzenia KRI*. Prezydent powierzył obowiązki: (1) Administratora Bezpieczeństwa Informacji Sekretarzowi Miasta Świdnicy, który jest odpowiedzialny za aktualizację, realizację i przestrzeganie PBI oraz (2) Administratora Systemów Informatycznych kierownikowi Referatu Informatyki i Informacji Publicznej, który odpowiedzialny jest za aktualizację, realizację i przestrzeganie instrukcji zarzadzania systemami informatycznymi. PBI poddawana była przeglądom doraźnie w sytuacji wystąpienia istotnych zmian. Ostatni przegląd PBI miał miejsce 12 czerwca 2014 r., a jego skutkiem była aktualizacja i wprowadzenie w dniu 23 czerwca 2014 r. zmian w PBI.

(dowód: akta kontroli str. 124-147, 150, 153-155, 210-211)

2.2. Kontrola wykazała, że inwentaryzacja zasobów informatycznych w Urzędzie była realizowana przy wykorzystaniu programu RADIX Środki Trwałe 2.18. Można tam było zidentyfikować komputery, które zostały losowo wybrane do badania – każda jednostka posiadała „Kartę: Środek trwały" zawierającą m.in. takie informacje jak: nazwa, nr inwentarzowy, data nabycie, miejsce użytkowanie, osoba odpowiedzialna, wartość początkowa, charakterystyka (w przypadku zestawów komputerowych: jednostka centralna, klawiatura, mysz, rodzaj systemu operacyjnego, rodzaj monitora). Ponadto konfiguracja techniczna komputerów i zainstalowane na nich oprogramowanie możliwe było do sprawdzenia za pomocą specjalistycznego oprogramowania z panelu administratora, które pozwala połączyć się z każdym komputerem pracującym w sieci wewnętrznej Urzędu.
Referat Informatyki i Informacji Publicznej prowadzi ewidencję oprogramowania i miejsce, w którym jest ono użytkowane oraz rejestr aktualizacji oprogramowania.

(dowód: akta kontroli str. 169-196, 200)

Kontrola zapobiegania możliwości zainstalowania nieautoryzowanego oprogramowania została dokonana na próbie 11 losowo wybranych komputerów[16]. W 10 przypadkach na stacjach roboczych nie można było zainstalować oprogramowania z poziomu jej Użytkownika. Na komputerze (laptopie) o numerze inwentarzowym PST/001325, użytkowanym przez dyrektor Departamentu Budżetowo-Finansowego, instalacja dostarczonego pliku przebiegła pomyślnie. Sekretarz Miasta Świdnica wyjaśniła, że dyrektor Departamentu Budżetowo-Finansowego jest administratorem Informatycznego Systemu BESTIA i realizując obowiązki sprawozdawczości budżetowej Gminy Miasta Świdnica często pracuje poza siedzibą Urzędu. W sytuacji koniecznej aktualizacji merytorycznego oprogramowania,

---

[14] Technika informatyczna. Techniki bezpieczeństwa. Systemy zarządzania bezpieczeństwem informacji oraz powiązanej z nią Polskiej Normy PN-ISO/IEC 17799:2007 Technika informatyczna. Techniki bezpieczeństwa. Praktyczne zasady zarządzania bezpieczeństwem informacji.

[15] Zarządzenie nr 120-37/2013 Prezydenta Miasta Świdnicy z dnia 16 maja 2013 r. w sprawie dokumentacji przetwarzania danych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne, zmienione Zarządzeniem nr 120-70/2013 Prezydenta Miasta Świdnicy z dnia 13 sierpnia 2013 r.

[16] Próba nie obejmowała sześciu komputerów otrzymanych w użyczenie z Ministerstwa Spraw Wewnętrznych i Administracji w ramach projektu „pl.ID - Polska ID karta", które były nieużywane przez Urząd.

umożliwiającej np.: wysyłkę czy przygotowanie sprawozdań, musi posiadać możliwość dokonania aktualizacji systemu BESTIA, co wymaga uprawnień administracyjnych. Dlatego laptop dyrektora włączono do grupy administracyjnej.

(dowód: akta kontroli str. 169, 200)

Ponadto w Urzędzie prowadzony był rejestr kontroli zgodności systemów teleinformatycznych z odpowiednimi normami i PBI oraz rejestr naruszeń legalności oprogramowania, w którym, w okresie kontroli, nie stwierdzono naruszenia legalności oprogramowania.

(dowód: akta kontroli str. 92-94)

2.3. Urząd w badanym okresie, na podstawie procedury zarządzania ryzykiem[17], przeprowadził dwie analizy ryzyka bezpieczeństwa informacji, co było zgodne z § 20 ust. 2 pkt 3 *rozporządzenia KRI*. W ich wyniku nie stwierdzono utraty poufności, dostępności oraz integralności informacji.

(dowód: akta kontroli str.216-234, 235-240)

2.4. Nadawanie/modyfikowanie/odbieranie uprawnień w ramach systemów informatycznych było uregulowane w oparciu o funkcjonujące w Urzędzie procedury[18]. O uprawnieniach pracowników w systemach informatycznych decydują ich przełożeni we wniosku złożonym do Administratora Bezpieczeństwa Informacji za pośrednictwem Administratora Systemów Informatycznych.
Przegląd uprawnień do systemów i zasobów informatycznych dokonano dla 15 losowo wybranych pracowników Urzędu. Stwierdzono, iż wszyscy oni posiadali uprawnienia adekwatne do realizowanych zadań określonych w zakresach obowiązków, co było zgodne z § 20 ust. 2 pkt 4 *rozporządzenia KRI*, oraz mieli sporządzone formalne wnioski o nadanie uprawnień do systemów IT zgodnie z obowiązującą w Urzędzie procedurą.

(dowód: akta kontroli str. 156-159, 209-215)

W toku kontroli sprawdzono zablokowania dostępu do systemów informatycznych dla byłych pracowników[19], którzy w okresie kontroli zakończyli pracę w Urzędzie. Badaniem objęto dostęp do kont pracowniczych w systemach wewnętrznych urzędu za pomocą programu NetWareAdministrator v.5.1.8 będącym sieciowym systemem operacyjnym. Stwierdzono, iż wszyscy wskazani pracownicy mieli zablokowane konta pracownicze i nie mieli dostępu do systemów wewnętrznych Urzędu, co było zgodne z § 20 ust. 2 pkt 4 *rozporządzenia KRI*. Przełożeni sporządzili stosowne wnioski o odebranie uprawnień użytkownikowi systemów informatycznych.

(dowód: akta kontroli str. 156-159, 203-206, 207-208)

2.5. W badanym okresie Urząd zapewnił szkolenia 65 pracownikom zaangażowanym w proces przetwarzania informacji (38% mających dostęp do systemów IT) w zakresie określonym w § 20 ust. 2 pkt 6 *rozporządzenia KRI*. Prezydent wyjaśnił, że „udział pracowników w szkoleniach wynikał z realnych potrzeb pracowników. Szkolenia nie były realizowane w oparciu o harmonogramy szkoleń na dany rok. Po upływie okresu urlopowego planowane jest przeprowadzenie kolejnego szkolenia w siedzibie Urzędu dla większej liczby pracowników zaangażowanych w przetwarzanie danych".

(dowód: akta kontroli str. 150-151)

---

[17] Procedura zarządzania ryzykiem w Urzędzie Miejskim w Świdnicy stanowiąca załącznik do zarządzenia nr 120-9/2011 Prezydenta Miasta Świdnicy z dnia 16 marca 2011 r., zmienione Zarządzeniem nr 120-67/2011 Prezydenta Miasta Świdnicy z dnia 28 grudnia 2011 r.

[18] Zarządzenie nr 120-15/2014 Prezydenta Miasta Świdnicy z dnia 14 lutego 2014 r. w sprawie procedury udostępniania pracownikom zasobów sieci LAN/WAN UM w Świdnicy.

[19] Na podstawie „Wykazu pracowników Urzędu Miejskiego w Świdnicy zwolnionych w latach 2012-2014".

2.6. W Urzędzie ustanowiono podstawowe zasady[20] w zakresie bezpiecznej pracy użytkowników przy wykorzystaniu komputerów przenośnych, zgodnie z § 20 ust. 2 pkt 8 *rozporządzenia KRI*. W myśl tych zasad pracownik użytkujący komputer przenośny zobowiązany jest do podłączenia komputera do sieci informatycznej Urzędu, bez określenia czasokresu na dokonanie tej czynności, w celu aktualizacji wzorców wirusów w programie antywirusowym oraz utrzymania konfiguracji oprogramowania systemowego w sposób wymuszający korzystanie z haseł. W zasadach tych określono też m.in. sposoby transportu komputera minimalizujące ryzyko jego kradzieży lub zniszczenia.

(dowód: akta kontroli str. 11, 142-144)

2.7. Zgodnie z obowiązującą procedurą[21] urządzenia, dyski lub inne elektroniczne nośniki informacji, przeznaczone do napraw w firmach zewnętrznych, pozbawia się w trwały sposób przed naprawą zapisu danych, albo naprawia się je pod nadzorem Administratora Systemów Informatycznych Urzędu.
W umowach serwisu oprogramowania/zakupu komputerów zawartych w okresie kontroli zostały wprowadzone stosowne zapisy dotyczące zabezpieczenia informacji, do których wykonawcy mogą mieć dostęp na etapie realizacji tych umów. W umowie serwisowej badanego oprogramowania firmy RADIX znalazły się zapisy dotyczące zobowiązania zleceniobiorcy do przestrzegania przepisów ujętych *w rozporządzeniu KRI*, co daje możliwości wszczęcia postępowania sądowego w przypadku niezachowania poufności informacji pozyskanych przez zleceniobiorcę w toku realizacji umowy. W umowie dostawy sprzętu komputerowego i oprogramowania zawarto zapisy zobowiązujące dostawcę do wykonywania napraw gwarancyjnych w miejscu instalacji sprzętu, czyli w Urzędzie, pod nadzorem pracowników Referatu Informatyki i Informacji Publicznej, a nośniki (dyski twarde komputerów) w razie uszkodzenia pozostają u zamawiającego. Działania powyższe były zgodne z § 20 ust. 2 pkt 10 *rozporządzenia KRI*.

(dowód: akta kontroli str. 141-142, 197, 199-202)

2.8. W Urzędzie, stosownie do § 20 ust. 2 pkt 13 *rozporządzenia KRI*, wprowadzono procedurę[22] nakazującą pracownikom niezwłoczne zgłaszanie Administratorowi Systemów Informatycznych incydentów naruszenia bezpieczeństwa informacji w sposób umożliwiający podjęcie działań korygujących. Z procedurą tą zostali zapoznani pracownicy Urzędu - w badanej próbie 15 pracowników, wszyscy podpisali stosowne oświadczenie.

(dowód: akta kontroli str. 11, 142)

2.9. W okresie objętym kontrolą, zgodnie z planem audytu na rok 2013, Urząd przeprowadził jeden audyt wewnętrzny z zakresu bezpieczeństwa informacji, co było zgodne z § 20 ust. 2 pkt 14 *rozporządzenia KRI*. Audyt został przeprowadzony przez firmę zewnętrzną. W jego wyniku powstał w październiku 2013 r. raport zawierający rekomendacje dla kierownictwa Urzędu, które wymagały podjęcia działań eliminujących bądź zmniejszających zdiagnozowane ryzyka. Rekomendacje dotyczyły wielu obszarów związanych z zabezpieczeniem systemów informatycznych,

---

[20] Pkt. XIII (Zasady korzystania z komputerów przenośnych) Instrukcji zarządzania systemami informatycznymi stanowiącej załącznik nr 2 do zarządzenia nr 120- 37/2013 Prezydenta Miasta Świdnicy z dnia 16 maja 2013 r. w sprawie dokumentacji przetwarzania danych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych.

[21] Pkt. XI (Procedury wykonywania przeglądów i konserwacji systemów oraz nośników informacji) Instrukcji zarządzania systemami informatycznymi stanowiącej załącznik nr 2 do zarządzenia nr 120-37/2013 Prezydenta Miasta Świdnicy z dnia 16 maja 2013 r.

[22] Pkt. XII (Procedury postępowania w sytuacji naruszenia ochrony danych) Instrukcji zarządzania systemami informatycznymi stanowiącej załącznik nr 2 do zarządzenia nr 120- 37/2013 Prezydenta Miasta Świdnicy z dnia 16 maja 2013 r.

koniecznością realizacji zapisów, właściwą oceną ryzyka, dokumentowaniem procedur, aktualizacją umów na serwis oprogramowania, opracowaniem wykazów, rejestrów i ewidencji wynikających z *rozporządzenia KRI*. Sformułowane w ramach przeprowadzonego audytu rekomendacje zostały zrealizowane. W Planie audytu na 2014 r. zaplanowano kolejny audyt wewnętrzny z zakresu bezpieczeństwa informacji.

(dowód: akta kontroli str. 11-12, 37-55, 57-90)

2.10. W Urzędzie wprowadzono procedurę tworzenia kopii bezpieczeństwa danych[23], w której określono zasady sporządzania i przechowywania kopii zapasowych danych oraz oprogramowania aplikacyjnego i ich częstotliwość.
Kopie zapasowe (backupy) baz danych wykonywane były automatycznie codziennie za pomocą programu MS SQL Server Management Studio oraz programu Cobian Backup 11 (dla pozostałych systemów informatycznych wraz z danymi z systemu elektronicznego obiegu dokumentów) i zapisywane na serwer backupowy. Każdy spakowany backup przed zapisem na nośnik był testowany pod kątem błędów i poprawnego spakowania oraz dokonywane było testowanie procedury odtworzeniowej.
Kopie zapasowe, zapisane na dyskach BD-R lub na dyskach twardych, zabezpieczone były i przechowywane w sposób należyty. Stan taki spełniał wymogi określone w § 20 ust. 2 pkt 12 lit. b *rozporządzenia KRI*, dzięki czemu minimalizowano ryzyko utraty informacji w wyniku awarii.

(dowód: akta kontroli str. 138-139, 241-251)

2.11. Badane systemy informatyczne udostępniały dane w następujących formatach:
- Systemie Usług Publicznych, poprzez Elektroniczną Platformę Usług Administracji Publicznej ePUAP, generuje pliki w formacie XML,
- System Windykacji Opłat i Podatków RADIX WIP+ generuje pliki w formacie RTF,
- System Gospodarowania Odpadami Komunalnymi RADIX GOK+, generuje pliki w formacie RTF,
- Systemu „Książka Drogi" z podsystemem „obiekty mostowe" generuje pliki w formatach: JPG, PDF, PNG, TIFF,

tj. zgodnie z wymogami określonymi w § 18 ust. 1 *rozporządzenia KRI*.

(dowód: akta kontroli str. 252, 263-265)

Uwagi dotyczące badanej działalności

1. NIK zauważa, iż przy dzisiejszym postępie technologicznym i mając na względzie zapewnienie PBI przydatności, adekwatności i skuteczności, PBI, zgodnie z zapisami pkt. 5.1.2. normy PN-ISO/IEC 17799:2007 powinna być poddawana regularnym przeglądom w zaplanowanych odstępach czasu lub w przypadku np. poważnego naruszenia bezpieczeństwa informacji, pojawienia się nowych i istotnych rodzajów ryzyka czy też zmian regulacji prawnych dotyczących bezpieczeństwa informacji. Zgodnie z dobrymi praktykami zaleca się aktualizowanie polityki bezpieczeństwa informacji nie rzadziej niż raz na sześć miesięcy.

2. NIK zwraca uwagę, że mając na uwadze możliwość odtworzenia informacji po katastrofie lub innym zdarzeniu losowym, niewystarczająca jest inwentaryzacja zasobów informatycznych na potrzeby finansowego rejestru środków trwałych i zaleca się stałe dysponowanie aktualnymi informacjami w zakresie posiadanego sprzętu informatycznego oraz jego konfiguracji, najlepiej prowadzonymi przez służby informatyczne Urzędu przy użyciu specjalistycznego oprogramowania. W ten sposób powinien być sporządzony i aktualizowany spis wszystkich aktywów informatycznych zawierający przede wszystkim informacje o jego rodzaju

[23] Pkt. VI (Procedury tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych) Instrukcji zarządzania systemami informatycznymi stanowiącej załącznik nr 2 do zarządzenia nr 120- 37/2013 Prezydenta Miasta Świdnicy z dnia 16 maja 2013 r.

i konfiguracji (np. pamięć RAM, pojemność dysku twardego, rodzaj karty graficznej, złącza zewnętrzne, system operacyjny, zainstalowane oprogramowanie). Należy też pamiętać, aby spis niepotrzebnie nie powielał innych spisów tworzonych w Urzędzie, jakkolwiek należy zapewnić ich wzajemną zgodność.

3. Zdaniem NIK w jak najkrótszym czasie wszyscy pracownicy Urzędu zaangażowani w proces przetwarzania informacji powinni zostać odpowiednio przeszkoleni oraz regularnie powiadamiani o zmianach w zakresie obowiązujących w Urzędzie polityk i procedur związanych z wykonywanymi przez nich zadaniami. Zapewnić to powinno, że wszyscy pracownicy będą świadomi zagrożeń i innych aspektów bezpieczeństwa informacji, swoich obowiązków i odpowiedzialności prawnej oraz będą minimalizować ryzyko błędów ludzkich.

4. Należy mieć na względzie, że regularne podłączenia komputerów przenośnych do lokalnej sieci komputerowej w celu aktualizacji oprogramowania pozwalają pracować na aktualnych ustawieniach systemu operacyjnego, w przeciwnym razie może to skutkować zmniejszeniem bezpieczeństwa informatycznego. Istotna jest również częstotliwość dokonywanych podłączeń. Wskazanym jest, aby obowiązek podłączenia przez pracowników komputera przenośnego do lokalnej sieci komputerowej odbywał się jak najczęściej. Biorąc pod uwagę, że rozprzestrzenianie zagrożeń informatycznych następuje niezwykle szybko, Urząd powinien wprowadzić przynajmniej miesięczny czas, w jakim pracownicy są zobowiązani podłączyć posiadany komputer przenośny do sieci lokalnej. Zdaniem NIK, zasadnym byłoby, aby następowało to w każdym dniu obecności pracownika w Urzędzie.

Ustalone nieprawidłowości

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

Ocena cząstkowa

Najwyższa Izba Kontroli ocenia pozytywnie działalność Urzędu w zakresie wdrożenia systemu zarządzania bezpieczeństwem systemów informatycznych.
Powyższą ocenę cząstkową uzasadniają ustalenia kontroli dotyczące w szczególności: [1] opracowania i wdrożenia do stosowania Polityki Bezpieczeństwa Informacji, [2] zablokowania możliwości swobodnego instalowania oprogramowania w posiadanych systemach informatycznych, [3] zawierania w umowach serwisu oprogramowania oraz zakupu komputerów postanowień mających gwarantować odpowiedni poziom bezpieczeństwa informacji, [4] zapewnienia audytu wewnętrznego w zakresie bezpieczeństwa informacji, [5] właściwego sposób przechowywania i zabezpieczenia kopii zapasowych danych.

3. Zapewnienie dostępności informacji dla osób niepełnosprawnych

Opis stanu faktycznego

W toku kontroli dokonano weryfikacji zgodności strony internetowej Urzędu[24] oraz strony BIP Urzędu[25] ze standardem WCAG 2.0. w zakresie Zasady 4 - Kompatybilność. W jej wyniku ustalono, iż:
- na stronie internetowej Urzędu wystąpiły dwa błędy i cztery ostrzeżenia stwierdzone przy badaniu z wykorzystaniem narzędzia dostępnego na stronie http://validator.w3.org,
- na stronie BIP Urzędu wystąpiły dwa błędy stwierdzone z wykorzystaniem narzędzia dostępnego na stronie http://jigsaw.w3.org/css-validator.

Wskazane wyżej błędy nie miały istotnego wpływu na prezentowanie treści dla osób niepełnosprawnych.

[24] http://um.swidnica.pl
[25] http:///www.swidnica.bip-gov.info.pl

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 tego rozporządzenia, czyli do dnia 30 maja 2015 r.

(dowód: akta kontroli str. 95-107)

IV. Uwagi i wnioski

Wnioski pokontrolne

Przedstawiając powyższe oceny i uwagi, wynikające z ustaleń kontroli, Najwyższa Izba Kontroli, na podstawie art. 53 ust. 1 pkt 5 ustawy z 23 grudnia 1994 r. *o Najwyższej Izbie Kontroli*[26] (dalej: *ustawa o NIK*), wnosi o:

1. Rozważenie możliwości formalnego wprowadzenia systemu elektronicznego prowadzenia spraw, jako podstawowego systemu wykonywania czynności kancelaryjnych w Urzędzie.
2. Objęcie sprawdzaniem przez specjalistyczne oprogramowanie inwentaryzujące wszystkich podłączonych do sieci Urzędu komputerów i urządzeń centralnych.
3. Podjęcie działań w celu przeszkolenia wszystkich pracowników Urzędu – zaangażowanych w proces przetwarzania informacji – w zakresie, o którym mowa w § 20 ust. 2 pkt 6 *rozporządzenia KRI*.
4. Wprowadzenie obowiązku podłączania komputerów przenośnych, co najmniej raz w okresie miesiąca, do lokalnej sieci komputerowej w celu aktualizacji oprogramowania.

V. Pozostałe informacje i pouczenia

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

Prawo zgłoszenia zastrzeżeń

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 we Wrocławiu.

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 wniosków pokontrolnych oraz o podjętych działaniach lub przyczynach niepodjęcia tych działań.

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.

Wrocław, dnia 30 września 2014 r.

Kontroler nadzorujący:
Artur Urban
Doradca ekonomiczny

.....
Podpis

Najwyższa Izba Kontroli
Delegatura we Wrocławiu
Dyrektor

DYREKTOR
Delegatura Najwyższej Izby Kontroli
we Wrocławiu

z up.
.....
Bogusław Florkowski
Wicedyrektor

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