NAJWYŻSZA IZBA KONTROLI
Delegatura w Szczecinie

LSZ – 4101-011-03/2014
P/14/004

WYSTĄPIENIE POKONTROLNE

NAJWYŻSZA IZBA KONTROLI
Delegatura w Szczecinie
ul. Jacka Odrowąża 1, 71-420 Szczecin
T +48 91 831 39 00, F +48 91 831 39 66
lsz@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 Szczecinie[1].

KontrolerKontroler

Bogumiła Mędrzak, główny specjalista kontroli państwowej, upoważnienie do kontroli nr 91868 z dnia 26 sierpnia 2014 r.

(dowód: akta kontroli str. 1-2)

Jednostka kontrolowana

Urząd Miasta Świnoujście[2], ul. Wojska Polskiego 1/5, 72-600 Świnoujście.

Kierownik jednostki kontrolowanej

Janusz Żmurkiewicz – Prezydent Miasta Świnoujście.

(dowód: akta kontroli str. 8)

II. Ocena kontrolowanej działalności

Ocena ogólna

Prezydent Miasta Świnoujście 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[3]:

- zapewnił współpracę wybranych do badania systemów informatycznych z innymi systemami Urzędu oraz z systemami innych jednostek administracji publicznej, co spełniało minimalne wymogi interoperacyjności, określone w § 5 ust. 3 pkt 3 rozporządzenia KRI;
- przeprowadził analizę zagrożeń występujących przy przetwarzaniu informacji i podjął działania w celu wyeliminowania stwierdzonego ryzyka, co było zgodne z § 20 ust. 2 pkt 3 rozporządzenia KRI;
- udostępnił katalog 22 usług świadczonych drogą elektroniczną, jednak w ocenie NIK nie podjął skutecznych działań w celu ułatwienia obywatelom korzystania z nich. Na stronach internetowych Urzędu i w Biuletynie Informacji Publicznej[4] nie zamieszczono linków do 16 z 22 usług realizowanych za pośrednictwem Elektronicznej Platformy Usług Administracji Publicznej[5], poprzestając na zamieszczeniu 6 linków do ogólnego przekierowania do ePUAP.

Ustalenia kontroli wykazały następujące nieprawidłowości przy realizacji zadań określonych w rozporządzeniu KRI:

- nie przeprowadzono inwentaryzacji sprzętu komputerowego, obejmującej ich rodzaj i konfigurację, co stanowiło naruszenie § 20 ust. 2 pkt 2 rozporządzenia KRI;

[1] Zwana dalej „NIK".

[2] Zwany dalej „Urzędem".

[3] Dz. U. z 2012 r., poz. 526, zwane dalej „rozporządzeniem KRI".

[4] Zwany dalej „BIP".

[5] Zwana dalej „e-PUAP".

- nie przestrzegano procedury odbierania uprawnień użytkownikom systemu EOD eKancelaria, co stanowiło naruszenie § 20 ust. 2 pkt 4 i 5 rozporządzenia KRI;
- nie przeszkolono w zakresie zachowania bezpieczeństwa informacji wszystkich pracowników zaangażowanych w proces przetwarzania informacji, co stanowiło naruszenie § 20 ust. 2 pkt 6 rozporządzenia KRI;
- pozostawiono możliwość zainstalowania nieautoryzowanego oprogramowania użytkownikom 15 badanych komputerów, nie będących pracownikami służb informatycznych, co stanowiło naruszenie § 20 ust. 2 pkt 7 lit. c rozporządzenia KRI;
- nie opracowano procedur gwarantujących bezpieczną pracę przy przetwarzaniu mobilnym i pracy na odległość, co stanowiło naruszenie § 20 ust. 8 rozporządzenia KRI*;*
- nie zawarto w umowach na serwisowanie 2 systemów informatycznych zapisów gwarantujących zabezpieczenie poufności informacji, co stanowiło naruszenie § 20 ust. 2 pkt 10 rozporządzenia KRI;
- nie przeprowadzono okresowego audytu wewnętrznego w zakresie bezpieczeństwa informacji, co stanowiło naruszenie § 20 ust. 2 pkt 14 rozporządzenia KRI.

W ocenie NIK zarządzanie bezpieczeństwem informacji, o którym mowa w rozporządzeniu KRI oraz w Polskiej Normie *Technika informatyczna. Techniki bezpieczeństwa. Systemy zarządzania bezpieczeństwem informacji* (PN-ISO/EIC 27001:2007)[6] było nierzetelne, a działania Prezydenta w zakresie wdrożenia systemu bezpieczeństwa systemów należy uznać za niewystarczające. NIK zwraca uwagę, ze chociaż Urząd był przygotowany do świadczenia usług elektronicznych[7], to nie podjął skutecznych działań zmierzających do popularyzacji komunikacji elektronicznej wśród obywateli.

III. Opis ustalonego stanu faktycznego

1. Dostosowanie systemów teleinformatycznych do współpracy z systemami innych podmiotów administracji publicznej

1.1. Elektroniczne świadczenie usług w dokumentach strategicznych gminy

Opis stanu faktycznego

W badanym okresie kierunki rozwoju Miasta Świnoujście zostały ujęte w trzech dokumentach planistycznych: Strategii Rozwoju Miasta Świnoujście (opracowanej w maju 2004 r.), w Strategii Rozwoju Miasta na lata 2014-2020 i Wieloletnich Strategicznych Programach Operacyjnych Miasta Świnoujście na lata 2014-2020.

W Strategii Rozwoju Miasta z 2004 r. zaplanowano rozwój infrastruktury teleinformatycznej i umiejętności posługiwania się narzędziami informatycznymi poprzez wdrożenie programu *eMiasto*. Zapis o wdrożeniu programu *eMiasto* był jedynym zapisem odnoszącym się do dostosowania jednostki do elektronicznego świadczenia usług publicznych i w żadnej części tego dokumentu nie został omówiony lub szerzej opisany. Nie określono zakresu działania programu, ani ram czasowych i wielkości wskaźnika (np. liczby udostępnionych usług) jakie zamierzano osiągnąć poprzez jego uruchomienie.

W Wieloletnich Strategicznych Programach Operacyjnych Miasta na lata 2014-2020 w ramach jednego z 4 celów strategicznych pn. *„Poprawa zewnętrznego i wewnętrznego systemu komunikacji i transportu”* zaplanowano rozwój systemów teleinformatycznych poprzez wdrożenie 3 zadań: 1) Szerokie świadczenie elektronicznych usług publicznych – w latach 2016-2017; 2) Wymiana dokumentów i informacji za pomocą elektronicznych środków komunikacji - w 2015 r.; 3) Zwiększenie dostępności i funkcjonalności systemów informacji przestrzennej w 2015 r.

Dla zaplanowanych zadań określono beneficjentów (tj. mieszkańców miasta i interesantów Urzędu, jednostki samorządu terytorialnego i miejskie spółki) oraz mierniki

[6] Zwanej dalej „Normą PN-ISO/EIC 27001:2007”.

[7] M.in. wprowadzenie systemu EOD eKancelaria zintegrowanego z ePUAP oraz prowadzenie korespondencji z innymi jednostkami administracji w sposób elektroniczny.

(tj. liczba udostępnionych systemów w instytucjach publicznych, liczba usług e-cyfrowych opartych na ponownym wykorzystaniu informacji sektora publicznego, liczba wejść na strony internetowe Urzędu i podległych mu jednostek, liczba osób korzystających z hot spotów).

(dowód: akta kontroli str. 40-54)

1.2. Promowanie komunikacji elektronicznej

Opis stanu faktycznego

Dokumenty planistyczne rozwoju Miasta, ani inne dokumenty nie zawierały informacji o sposobach promowania komunikacji elektronicznej przez Urząd lub przez Kierownika jednostki. W Urzędzie nie przyjęto i nie wdrażano programu promocji w ww. zakresie.

(dowód: akta kontroli str. 40-54)

Pan Janusz Żmurkiewicz - Prezydent Miasta Świnoujście[8] wyjaśnił m.in.: *Urząd zachęca klientów do korzystania z ePUAP. Na stronie internetowej Urzędu w dniu 25.07.2011 r. pojawił się artykuł „Uwaga! Nie trzeba już przychodzić do urzędu", gdzie zareklamowano możliwość i opisano sposób korzystania ze zdalnego załatwiania spraw.*

(dowód: akta kontroli str. 191-200)

1.3. Ankiety lub inne formy poznania potrzeb mieszkańców gminy odnośnie elektronicznej formy komunikacji

Opis stanu faktycznego

W badanym okresie Urząd nie dokonywał analiz dotyczących poznania potrzeb mieszkańców i turystów w zakresie elektronicznej formy komunikacji z Urzędem.

Zarządzeniem Nr 663/2009 Prezydenta Miasta Świnoujście z dnia 1.10.2009 r. w sprawie ustalenia procedury badania poziomu zadowolenia interesantów z usług świadczonych przez Urząd Miasta Świnoujście, wprowadzono możliwość złożenia przez mieszkańców i turystów ankiety na temat jakości usług świadczonych w Urzędzie. Ankietę można było złożyć papierowo w siedzibie Urzędu lub za pośrednictwem poczty elektronicznej (formularz ankiety zamieszczono na stronie internetowej Urzędu). Żadne z pytań zawartych w formularzu ankiety nie dotyczyło opinii oraz potrzeb interesantów w zakresie elektronicznej formy komunikacji z Urzędem.

(dowód: akta kontroli str. 6-7, 34-39)

Uwagi dotyczące badanej działalności

W ocenie NIK poznanie potrzeb i oczekiwań obywateli w zakresie dostępności do usług elektronicznych jest warunkiem zapewnienia sprawnego świadczenia takich usług przez Urząd. Zwiększenie udziału komunikacji elektronicznej w świadczeniach publicznych realizowanych przez Urząd, zorientowanie na rozwój i poszerzenie usług elektronicznych pozwoliłoby na usprawnienie pracy Urzędu.

1.4. Korespondencja z Ministrem Administracji i Cyfryzacji[9]

Opis stanu faktycznego

Po wejściu w życie w dniu 31.05.2012 r. rozporządzenia KRI, Urząd nie zwracał się do Ministra Administracji i Cyfryzacji z problemami lub z prośbą o pomoc w zakresie dostosowania swoich systemów i rejestrów informatycznych do wymogów Krajowych Ram Interoperacyjności[10].

(dowód: akta kontroli str. 6-7, 23)

1.5. Procedury regulujące komunikację elektroniczną w Urzędzie

Opis stanu faktycznego

W badanym okresie podstawowym sposobem dokumentowania przebiegu załatwiania i rozstrzygania spraw w Urzędzie był tradycyjny („papierowy") system wykonywania czynności kancelaryjnych wprowadzony zarządzeniem Nr 279/2011 Prezydenta Miasta Świnoujście z dnia 29.04.2011 r. W § 1 ww. zarządzenia określono, że system tradycyjny

[8] Zwany dalej „Prezydentem".

[9] Zwany dalej „MAiC".

[10] Zwane dalej „KRI".

wykonywania czynności kancelaryjnych może być wspomagany przez korzystanie z narzędzi informatycznych w procesie obiegu dokumentacji.

(dowód: akta kontroli str. 6-7, 32-33)

W regulaminach organizacyjnych Urzędu[11] obowiązujących w badanym okresie określono, że zasady i tryb wykonywania czynności kancelaryjnych określają właściwe przepisy.

W § 68 obowiązującego regulaminu organizacyjnego określono, że ewidencję korespondencji przychodzącej prowadzi Stanowisko Obsługi Interesantów, a całokształt spraw związanych z przyjmowaniem, rejestrowaniem i kolportowaniem korespondencji wychodzącej z Urzędu należy do Wydziału Organizacyjnego.

(dowód: akta kontroli str. 87-89, 125)

Od 17.12.2012 r. Urząd rozpoczął wykorzystywanie systemu EOD e-Kancelaria do wspomagania procesu obiegu dokumentów.

(dowód: akta kontroli str. 193)

Czynności kancelaryjne w EOD eKancelaria wykonywano zgodnie z przepisami rozporządzenia w sprawie Instrukcji Kancelaryjnej, w następujący sposób:

- pisma składane przez klientów za pomocą ePUAP były automatycznie przekierowywane do systemu EOD eKancelaria, następnie rejestrowane i przesyłane w systemie do adresatów wskazanych w pismach (tj. Prezydenta lub Naczelników Wydziałów/Kierowników Biur);
- dekretację danego pisma w systemie dokonywał Prezydent lub Naczelnicy Wydziałów/Kierownicy Biur, a następnie przekazywał w systemie do właściwego Wydziału/Biura lub pracownika (wg kompetencji określonych w regulaminie organizacyjnym lub w Karcie zakresu obowiązków, uprawnień i odpowiedzialności pracowników);
- po przygotowaniu odpowiedzi (poza systemem EOD eKancelaria) Naczelnicy Wydziału/Kierownicy Biur lub właściwi pracownicy przesyłali za pośrednictwem systemu pismo (poprzez pobranie pliku) do Prezydenta (jego zastępców i Skarbnika) do akceptacji oraz w celu złożenia podpisu elektronicznego. Po podpisaniu elektronicznie przez Prezydenta (jego zastępców lub Skarbnika) dokument wysyłano odbiorcy z użyciem systemu EOD eKancelaria za pośrednictwem ePUAP.

System EOD eKancelaria zapewniał funkcjonalność w zakresie akceptacji (weryfikacji) pisma stanowiącego odpowiedź w danej sprawie.

(dowód: akta kontroli str. 207-208, 211-218)

Uwagi dotyczące badanej działalności

W wewnętrznych procedurach Urzędu dotyczących wykonywania czynności kancelaryjnych nie określono zasad obiegu dokumentów wpływających do Urzędu drogą elektroniczną oraz zasad wykorzystywania systemu informatycznego EOD e-Kancelaria do wspomagania procesu obiegu dokumentów (wprowadzonego w Urzędzie od grudnia 2012 r.). Zdaniem NIK ze względu na znaczące wykorzystanie systemu informatycznego EOD e-Kancelaria w procesie obiegu dokumentów w Urzędzie, zasadnym jest opracowanie odpowiednich instrukcji obiegu dokumentów uwzględniających przyjętą praktykę postępowania.

(dowód: akta kontroli str. 55-129)

Pan Jerzy Lenda - Sekretarz Miasta[12] wyjaśnił, że w *Urzędzie obowiązuje tradycyjny system wykonywania czynności kancelaryjnych, z możliwością korzystania z narzędzi informatycznych do wspomagania procesu obiegu dokumentacji. Zostało to uregulowane Zarządzeniem Nr 279/2011 Prezydenta Miasta Świnoujście z dnia 29.04.2011 r. System jest oparty na jednolitym rzeczowym wykazie akt wprowadzonym rozporządzeniem w sprawie*

[11] Wprowadzonych zarządzeniem Nr 216/2011 Prezydenta Miasta Świnoujście z 31.03. 2011 r. (zmienionym zarządzeniem Nr 14/2012 z dnia 12.01 2012 r., zarządzeniem Nr 516 z 14.09.2012 r. i zarządzeniem Nr 654/2012 z 27.11.2012 r) oraz zarządzeniem Nr 492/2013 z 1.08.2013 r. (zmienionym zarządzeniem Nr 815/2013 z 31.12 2013 r. oraz zarządzeniem Nr 434/2014 z 15.07.2014 r.).

[12] Sprawujący bezpośredni nadzór pracy Kierownika Biura Technologii Informacyjnych – zwany dalej „Sekretarzem Miasta".

Instrukcji Kancelaryjnej. Obecnie trwają prace i konsultacje nad opracowaniem instrukcji obiegu dokumentów (z wykorzystaniem systemów teleinformatycznych do elektronicznego zarządzania dokumentacją).

(dowód: akta kontroli str. 9-12, 32, 438-442)

1.6. Liczba złożonych dokumentów / wniosków / podań

Opis stanu faktycznego

W okresie od 31.05.2012 r. do 31.05.2014 r. obywatele złożyli do Urzędu 54.937 dokumentów, w tym 249 - w formie elektronicznej (0,4%), a 54.688 – w formie papierowej. W ww. okresie podmioty gospodarcze złożyły 46.200 dokumentów (w tym 533 - w formie elektronicznej (1,1%) i 45.667 - w formie papierowej), a inne urzędy - 59.941 dokumentów (w tym 3.348 - formie elektronicznej (5,6%), a 56.593 - w formie papierowej).

(dowód: akta kontroli str. 206)

1.7. Zgodność opisu usług elektronicznych z usługami Urzędu

Opis stanu faktycznego

Według stanu na 30.05.2012 r. (tj. przed wejściem w życie rozporządzenia KRI) Urząd świadczył 27 usług elektronicznych, a po 31.05.2012 r. – zaktualizował wykaz faktycznie świadczonych usług do 22. Obywatel miał możliwość złożenia m.in.: wniosku o prawo jazdy; zawiadomienia o odkryciu zabytku; wniosku o udzielenie bonifikaty od opłaty rocznej z tytułu użytkowania wieczystego; wniosku o objęcie patronatem imprez o charakterze lokalnym i ponadlokalnym; wniosku o udostępnienie rejestru wyborców; dowolnego wniosku do urzędu.

(dowód: akta kontroli str. 193-199)

Według stanu na 16.09.2014 r. Urząd udostępnił 22 usługi elektroniczne za pośrednictwem ePUAP. Badaniem objęto 5 z 22 usług elektronicznych udostępnionych przez Urząd za pomocą ePUAP, tj.:

- wniosek o prawo jazdy;
- zawiadomienie o odkryciu zabytku;
- wniosek o udzielenie bonifikaty od opłaty rocznej z tytułu użytkowania wieczystego;
- wniosek o objęcie patronatem imprez o charakterze lokalnym i ponadlokalnym;
- wniosek o udostępnienie rejestru wyborców.

Wszystkie badane usługi elektroniczne były zgodne z usługami faktycznie świadczonymi przez Urząd oraz zawierały formularz i dane dotyczące podmiotu realizującego usługę elektroniczną (Urząd Miasta Świnoujście), miejsce świadczenia usługi –- siedziba Urzędu, osoby uprawnione do otrzymania usługi, wymagane dokumenty, czas i sposób realizacji usługi, opłaty i podstawę prawną.

(dowód: akta kontroli str. 141-177)

Za pośrednictwem strony internetowej Urzędu (www.swinoujscie.pl) zakładki E-Urząd - odsyłającej do strony internetowej Urzędu w BIP (http://bip.um.swinoujscie.pl/?cid=3091 w zakładce „Elektroniczna skrzynka podawcza") – Urząd udostępnił dla obywateli 6[13] z 22 usług elektronicznych świadczonych za pośrednictwem e-PUAP poprzez zamieszczenie linków do danej usługi[14]. Dla pozostałych 16 usług świadczonych za pomocą ePUAP, Urząd nie zamieścił na stronie internetowej Urzędu oraz w BIP informacji o możliwości złożenia pism poprzez ePUAP, ani linków do odpowiednich formularzy tych usług. Aby uzyskać do nich dostęp należało wejść bezpośrednio na stronę www.epuap.gov.pl i z użyciem opcji wyszukiwania odnaleźć usługi świadczone w gminie Świnoujście.

(dowód: akta kontroli str. 130-131, 141-177)

[13] Wniosek o prawo jazdy; zawiadomienie o odkryciu zabytku; wniosek o udzielenie bonifikaty od opłaty rocznej z tytułu użytkowania wieczystego; wniosek o objęcie patronatem imprez o charakterze lokalnym i ponadlokalnym; wniosek o udostępnienie rejestru wyborców; złożenie dowolnego wniosku do urzędu.

[14] Odsyłającego do e-PUAP.

Prezydent wyjaśnił m.in.: *Na stronie internetowej Urzędu oraz w BIP nie zamieszczono wszystkich usług z powodu braku zainteresowania interesariuszy Urzędu wykorzystywaniem formularzy umieszczonych na ePUAP. Od 29.11.2010 r., od kiedy to formularze zostały zainstalowane na ePUAP, do Urzędu wpłynęło w sumie tylko 6 wniosków wykorzystujących formularze. Były to: Wniosek EDG-1, Wniosek o wznowienie działalności, Wniosek o zmianę danych, Wniosek o dopisanie do listy wyborców, Wniosek o udostępnienie rejestru wyborców, Wniosek o objęcie patronatu. Dla interesariuszy Urzędu, w poprzedniej odsłonie ePUAP wszystkie rodzaje usług elektronicznych, udostępnianych przez Urząd były znacznie bardziej czytelne. Wówczas, chcąc skorzystać z usług elektronicznych wystarczyło wpisać nazwę Urząd i podane były wszystkie usługi udostępniane przez konkretny Urząd. Nowa odsłona ePUAP jest znacznie bardziej awaryjna, posiada zbyt wiele wyników wyszukiwanie usług, gdyż pojawiają się usługi nie tylko z Urzędu a i z innych jednostek (wyszukiwanie nie jest zawężone), co zniechęca potencjalnych usługobiorców. Najczęściej wykorzystywanym formularzem przez interesariuszy prywatnych Urzędu jest formularz „Złożenie dowolnego wniosku do Urzędu", gdyż wystarczy załączyć do tego wniosku dowolne pismo, zeskanowany formularz papierowy. Dokumenty w postaci elektronicznej opatrzone podpisem potwierdzonym profilem zaufanym ePUAP są równoważne pod względem skutków prawnych dokumentowi opatrzonemu podpisem własnoręcznym.*

(dowód: akta kontroli str. 191-199)

Ponadto, na stronie internetowej Urzędu (www.swinoujscie.pl) w zakładce „Załatw sprawę w Urzędzie" odsyłającej do strony internetowej w BIP zakładki „Wykaz spraw i sposób załatwienia" (http://bip.um.swinoujscie.pl/ index.php?cid=59) zamieszono wg wykazu spraw rozpatrywanych przez Urząd linki do pobrania plików w zakresie danej usługi (w których zamieszczono opis i sposób załatwienia danej usługi). Na stronie w BIP znajdował się opis 1 z 5 badanych usług świadczonych elektronicznie, tj. o wydanie prawa jazdy po raz pierwszy.

(dowód: akta kontroli str. 138-177)

1.8. Opisy procedur elektronicznego załatwiania spraw w BIP

Opis stanu faktycznego

Na stronie internetowej BIP w zakładce „Elektroniczna skrzynka podawcza" (http://bip.um.swinoujscie.pl/index.php?cid=3091) Urząd zamieścił informację o obowiązujących procedurach w zakresie załatwiania spraw drogą elektroniczną.

Urząd udostępniał na stronie internetowej w BIP 6 z 22 usług elektronicznych świadczonych za pomocą ePUAP poprzez zamieszczenie linków do tych usług. Linki odsyłały do ogólnej strony ePUAP zakładki „Załatw sprawę przez Internet", odnoszącej się do wszystkich kategorii spraw załatwianych za pomocą ePUAP. Zakładka ta nie odnosiła się bezpośrednio do opisu i formularza sprawy zawartej w linku (realizowanej przez Urząd elektronicznie).

(dowód: akta kontroli str. 130-131, 141-143)

Sekretarz Miasta wyjaśnił*: Linki do poszczególnych usług dostępnych na ePUAP były zamieszczone na stronie BIP Urzędu i działały poprawnie. Niestety, aktualizacja wyglądu portalu przez właściciela platformy spowodowała, że linki do usług przestały działać. Aktualizacja ePUAP nie powinna likwidować połączeń pomiędzy stronami Urzędu a usługami na platformie, gdyż niepotrzebnie wymusza powtórne wykonanie tej samej pracy. Obecnie linki przenoszą interesariusza do ePUAP, choć nie do konkretnej usługi. Podjęto działania zmierzające do poprawy takiego stanu i wkrótce linki zostaną powtórnie połączone z odpowiednimi usługami.*

(dowód: akta kontroli str. 447-458)

W BIP znajdował się opis 1 z 5 badanych usług świadczonych elektronicznie[15], tj. o wydanie prawa jazdy po raz pierwszy, który był zgodny z opisem usługi zamieszczonym w ePUAP,

[15] Wniosek prawa jazdy; zawiadomienie o odkryciu zabytku; wniosek o udzielenie bonifikaty od opłaty rocznej z tytułu użytkowania wieczystego; wniosek o objęcie patronatem imprez o charakterze lokalnym i ponadlokalnym; wniosek o udostępnienie rejestru wyborców.

poza danymi w zakresie przywołaniem podstawy prawnej (na ePUAP przywołano 19 podstaw prawnych wydania prawa jazdy, a w BIP – 5). W BIP nie zamieszczono opisu pozostałych 4 badanych usług (tj. zawiadomienia o odkryciu zabytku; wniosku o udzielenie bonifikaty od opłaty rocznej z tytułu użytkowania wieczystego; wniosku o objęcie patronatem imprez o charakterze lokalnym i ponadlokalnym; wniosku o udostępnienie rejestru wyborców).

(dowód: akta kontroli str. 134-137, 141-151, 174)

Na stronie internetowej w BIP w zakładce „Druki i wnioski do pobrania" (http://bip.um.swinoujscie.pl/index.php?cid= 2887) zamieszczono linki do pobrania plików stanowiących formularze danej sprawy. Na stronie w BIP nie zamieszczono formularzy do 5 badanych usług świadczonych elektronicznie za pomocą ePUAP (tj. wniosku o wydanie prawa jazdy; zawiadomienia o odkryciu zabytku; wniosku o udzielenie bonifikaty od opłaty rocznej z tytułu użytkowania wieczystego; wniosku o objęcie patronatem imprez o charakterze lokalnym i ponadlokalnym, wniosku o udostępnienie rejestru wyborców).

(dowód: akta kontroli str. 138-140, 141-143)

Prezydent wyjaśnił m.in.: *Urząd nie zamieścił opisu usług na stronie internetowej Urzędu w BIP w zakładce „Wykaz spraw i sposób załatwienia" przez przeoczenie. Urząd nie zamieścił formularzy dokumentów dotyczących usług elektronicznych na stronie internetowej Urzędu w BIP w zakładce „Druki i wnioski do pobrania" przez przeoczenie. Przy czym złożenie dowolnego wniosku do urzędu dotyczy wyłącznie platformy elektronicznej. Klient Urzędu nie musi składać dowolnego wniosku na formularzu. Opis procedur, w tym także podstaw prawnych usług elektronicznych realizowanych przez Urząd za pomocą ePUAP nie był aktualizowany. Brak aktualizacji wynikał z wykonywania dużej ilości innych zadań oraz braku rzeczywistego zainteresowania interesariuszy Urzędu używaniem tej formy załatwiania spraw w Urzędzie. Do Urzędu nie wpłynął żaden wniosek w formie elektronicznej o wydanie prawa jazdy, mimo że udostępniony jest już od 4 lat.*

(dowód: akta kontroli str. 191-199)

1.9. Przekazanie wzorów dokumentów elektronicznych do centralnego repozytorium wzorów dokumentów elektronicznych na ePUAP

Opis stanu faktycznego

Prezydent Miasta Świnoujście nie przekazał do centralnego repozytorium na ePUAP wzorów dokumentów elektronicznych, o których mowa w art. 19b ust. 3 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne[16], gdyż skorzystał z wzorów dokumentów elektronicznych udostępnionych przez Ministerstwo Gospodarki, Centrum Projektów Informatycznych oraz Ministerstwo Spraw Wewnętrznych i Administracji.

(dowód: akta kontroli str. 191-199)

1.10. Wspieranie modelu usługowego w zakresie świadczenia usług elektronicznych

Opis stanu faktycznego

Strona internetowa Urzędu działa pod adresem www.swinoujscie.pl, a strona internetowa w BIP - pod adresem http://bip.um.swinoujscie.pl/. Na stronie www Urzędu zamieszczono linki do stron BIP oraz stron ePUAP za pośrednictwem linka E-URZĄD. Urząd nie wykorzystywał innej strony internetowej do świadczenia usług elektronicznych.

(dowód: akta kontroli str. 141-143, 193)

Urząd w procesie zarządzania usługami elektronicznymi w podstawowym zakresie wspiera model usługowy. W odniesieniu do wszystkich 5 badanych usług udostępnionych elektronicznie za pomocą ePUAP można zidentyfikować jednostkę organizacyjną świadczącą usługi oraz zamieszczono karty opisu usługi (nie były one aktualizowane po 31.05.2012 r.). W stosunku do żadnej z usług nie wskazano maksymalnego czasu

[16] Dz. U. z 2013 r., poz. 235 ze zm.

niedostępności usługi, sposobu zgłaszania awarii, technicznego właściciela usługi (ePUAP), nie wskazano dopuszczalnych okresów niedostępności usługi elektronicznej.

(dowód: akta kontroli str. 141-177, 198-199)

Zgodnie z definicją zawartą w § 2 pkt 8 rozporządzenia KRI, model usługowy jest modelem architektury systemu informatycznego, w którym dla użytkowników zdefiniowano stanowiące odrębną całość funkcje systemu teleinformatycznego oraz opisano sposób korzystania z tych funkcji.

Prezydent wyjaśnił m.in.*, że w opisie usługi nie został wskazany maksymalny czas niedostępności, sposób zgłaszania awarii, podmioty odpowiedzialne za usuwanie awarii, techniczny właściciel usługi, gdyż wszystkie usługi są udostępnione na ePUAP i wszystkie parametry dostępności zależą wyłącznie od dostępności platformy, której właścicielem jest MAiC. Nie zostały określone dopuszczalne okresy niedostępności usługi elektronicznej, gdyż okresy te zależą ściśle od dostępności platformy, której właścicielem jest MAiC.*

(dowód: akta kontroli str. 191-199)

1.11. Współpraca wybranych systemów informatycznych z innymi systemami

Opis stanu faktycznego

Zakres i sposób współpracy systemów informatycznych wewnątrz Urzędu oraz ich współpracy z systemami zewnętrznymi (m.in. innych jednostek administracji publicznej) zbadano na próbie czterech systemów tj.:

1) Systemu EOD e-Kancelaria - służącego do elektronicznego ewidencjonowania i obiegu dokumentów.
2) Systemu Odpady w Gminie - odpadywgminie.com[17] - służącego do obsługi systemu gospodarki opadami.
3) Systemu Informacji Przestrzennej Geo-Info[18] - służącego m.in. do gromadzenia danych w zakresie geodezyjnej sieci uzbrojenia terenu, podziału i scaleń działek.
4) Systemu FORIS Zarządzanie Transportem Publicznym[19] służącego m.in. do ewidencji danych związanych z wydawaniem licencji, zezwoleń i zaświadczeń dotyczących transportu krajowego.

System EOD eKancelaria współpracował na poziomie dwustronnej komunikacji[20] z systemem ePUAP[21] - dane w zakresie korespondencji z ePUAP przekazywane były do systemu eKancelaria (i odwrotnie).

(dowód: akta kontroli str. 207-208)

System **odpadywgminie.com** współpracował z dwoma systemami informatycznymi na poziomie jednostronnej komunikacji[22] - z systemem bankowym (poprzez zaczytanie pliku csv przez pracownika Urzędu) oraz z systemem finansowo-księgowym[23] (poprzez eksport danych z systemu odpadywgminie.com i import tych danych do Zintegrowanego Systemu Ratusz[24] - przez pracownika w Wydziale Księgowości)[25].

(dowód: akta kontroli str. 219-228)

---

[17] Zwany dalej „System opadywgminie.com".

[18] Zwany dalej „System Geo-Info".

[19] Zwany dalej „System FORIS".

[20] 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.

[21] Dane z jednego systemu informatycznego przekazywane są do innego systemu, wymagane jest zatwierdzenie wyników przez operatora, odpowiedź z systemu jest przekazywana analogicznie.

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

[23] tj. Zintegrowanym Systemem Ratusz.

[24] Zwany dalej „ZS Ratusz".

[25] W zakresie danych dotyczących opłat za odpady.

System Geo-Info współpracował na poziomie jednostronnej komunikacji z wewnętrznym Systemem Informacji o Terenie - w zakresie przekazywania danych graficznych zgromadzonych w Module Geo-Info Mapa (pozyskiwanych z wyeksportowanego pliku w formacie TANGO, zawierającego informacje o przebiegu granic działek ewidencyjnych, klasoużytków oraz obrysów budynków itp.) oraz danych opisowych zgromadzonych w Module Integra (pozyskiwanych z ewidencji gruntów i budynków poprzez zadanie zdefiniowane DTS zaplanowane do wykonania na serwerze MS SQL Server).

Ponadto, system Geo-Info współpracował na poziomie jednostronnej komunikacji z ZS Ratusz (poprzez import pliku swde przez administratora ZS Ratusz) oraz na poziomie transakcyjnym[26] z systemem zewnętrznym GEOPORTAL, który obsługuje bazy Głównego Geodety Kraju (generowane i eksportowane przez Geo-Info pliki wymiany przekształcane programem MAP-serwer na pliki WMS - pobierane automatycznie przez system GEOPORTAL).

(dowód: akta kontroli str. 234-238)

Według stanu na 18.09.2014 r. **system FORIS** (Moduł Dokumenty) nie współpracował z żadnym zewnętrznym ani wewnętrznym systemem informatycznym Urzędu. Służył on do ewidencji danych związanych z wydawaniem licencji, zezwoleń i zaświadczeń dotyczących transportu krajowego (m.in. licencji na przewóz osób taksówką, zezwolenia na wykonywanie zawodu przewoźnika drogowego, licencji na pośrednictwo przy przewozie rzeczy (spedycja), poprzez ręczne uzupełnianie poszczególnych formatek dla danego rodzaju spraw).

(dowód: akta kontroli str. 229-233)

Sekretarz Miasta wyjaśnił m.in.: *System FORIS nie współpracuje z żadnym systemem wewnętrznym Urzędu, gdyż zawiera dane referencyjne, które są przekazywane do systemu zewnętrznego Centralnej Ewidencji i Informacji o Działalności Gospodarczej[27]. Po powtórnej analizie funkcjonalności systemu FORIS, wykazano możliwość współpracy systemem ogólnokrajowym – portalem CEIDG. Od 1.10.2014 roku będzie stosowane zasilanie bazy informacjami z systemu FORIS , m.in o numerze licencji dla przewoźnika TAXI. W zakładce „Raporty" w segmencie „Przewoźnicy" po wyborze z listy raportów „Plik do CEIDG", dane są generowane i eksportowane do pliku w formacie XML. Uprawniony pracownik do współpracy z CEIDG, po zalogowaniu na portalu, może importować dane do bazy CEIDG, z wcześniej przygotowanego pliku systemem FORIS.*

(dowód: akta kontroli str. 447-458, 486)

1.12. Procedury i praktyki postępowania stosowane we współpracy z innymi jednostkami administracji publicznej

Opis stanu faktycznego

W badanym okresie Urząd prowadził komunikację elektroniczną z dwoma jednostkami administracji publicznej: Zachodniopomorskim Urzędem Wojewódzkim[28] oraz Urzędem Statystycznym w Szczecinie (które wystąpiły z wnioskiem do Prezydenta o wymianę danych pomiędzy jednostkami w formie elektronicznej).

Od 2008 r. rozpoczął komunikację elektroniczną z Urzędem Statystycznym w Szczecinie w zakresie przekazywania sprawozdań, a od 2013 r. z ZUW w zakresie przekazywania pism w postępowaniach administracyjnych prowadzonych przez Wojewodę Zachodniopomorskiego, w których Miasto Świnoujście było stroną.

(dowód: akta kontroli str. 178-190)

Sekretarz Miasta wyjaśnił m.in., *że Urząd nie występował do innych jednostek administracji publicznej w celu wprowadzenia elektronicznej komunikacji wyłącznie w formie elektronicznej. Systemy informatyczne w Urzędzie wymieniają dane wyłącznie w sposób elektroniczny z różnymi niżej wymienionymi systemami w administracji publicznej:*

[26] Wymiana danych pomiędzy systemami odbywa się w sposób w pełni zautomatyzowany.

[27] Zwany dalej „CEIDG".

[28] Zwany dalej „ZUW".

1. *ePUAP – przekazywanie i przyjmowanie uwierzytelnionych danych m.in. od ZUW, Urzędów Skarbowych, interesariuszy Urzędu.*
2. *Portal GUS – wszystkie sprawozdania jednostek samorządu terytorialnego przekazuje w formie elektronicznej.*
3. *Programu Płatnik - dokumenty rozliczeniowe i ubezpieczeniowe, wymiana informacji z Zakładem Ubezpieczeń Społecznych.*
4. *Portal e-PFRON przekazywanie deklaracji i informacji o składkach na rzecz PFRON.*
5. *Platforma eDeklaracje – przesyłanie informacji o uzyskanych przychodach do Urzędów Skarbowych.*
6. *Platformy ogłoszeń zamówień publicznych: Biuletynu Urzędu Zamówień Publicznych, SIMAP - System Informacyjny Europejskich Zamówień Publicznych, Platforma Licytacji Elektronicznych, BIP Urzędu.*
7. *Portal Informacyjny Administracji – przez platformę wymiany informacji przesyłane są zawiadomienia o zmianach w zameldowaniu, aktualizacji danych osobowych.*
8. *System Wydawania Dowodów Osobistych.*
9. *Przekazywanie sprawozdań dotyczących budżetu poprzez system Besti@ (System Zarządzania Budżetem Jednostek Samorządu Terytorialnego) oraz ePUAP: RB-27S, Rb-28S, Rb-NDS, Rb-WSa, Rb-N, Rb-Z, Rb-PDP, Rb-UZ, Rb-UN, Rb-ST, bilans skonsolidowany, roczne sprawozdanie finansowe, Rb-50, Rb-30S, Rb-34S, Rb-27ZZ, Rb-ZN, Rb-28NWS.*
10. *Portal Karta Dużej Rodziny (ewidencja), Centralna Aplikacja Statystyczna (sprawozdawczość).*
11. *Platforma wyborcza.*
12. *Publikowanie aktów prawa miejscowego w Dzienniku Urzędowym ZUW.*
13. *Centralna Ewidencja Pojazdów i Kierowców – w prowadzonych postępowaniach identyfikowanie danych właścicieli pojazdów na postawie numerów rejestracyjnych pojazdów.*
14. *Elektroniczne przelewy masowe, zaczytywanie do systemów Wirtualnych Numerów Rachunków Bankowych (podatek od nieruchomości, opłaty za gospodarowanie odpadami).*
15. *Portal CEIDG - pomoc przedsiębiorcom w rejestracji działalności gospodarczej.*
16. *Portal Krajowa Baza Azbestowa – przekazywanie informacji o lokalizacji azbestu.*

(dowód: akta kontroli str. 6-7, 24-25)

Ocena cząstkowa

Najwyższa Izba Kontroli ocenia pozytywnie działalność Urzędu w zakresie dostosowania posiadanych systemów teleinformatycznych do współpracy z systemami używanymi przez inne podmioty administracji publicznej. Wymiana informacji z ZUW, Urzędem Statystycznym w Szczecinie oraz z kilkoma innymi urzędami odbywała się w formie elektronicznej. System wewnętrznego obiegu dokumentów (EOD eKancelaria) został zintegrowany z ePUAP. Mimo że, nie zamieszczono na stronach internetowych Urzędu i w BIP informacji o 16 z 22 usług elektronicznych świadczonych za pomocą ePUAP, skorzystanie z tych usług było możliwe poprzez wykorzystanie narzędzi zamieszczonych na ePUAP (opisanych na stronach internetowych Urzędu i w BIP).

W ocenie NIK umieszczenie pełnej informacji o świadczonych usługach elektronicznych na stronach internetowych Urzędu i w BIP może wpłynąć na większe zainteresowanie klientów tą formą komunikacji z Urzędem.

2. Zarządzanie bezpieczeństwem systemów informatycznych

2.1. Dokumenty z zakresu bezpieczeństwa informacji

Opis stanu faktycznego

W badanym okresie w Urzędzie obowiązywała wewnętrzna procedura dotycząca bezpieczeństwa informacji w zakresie przetwarzania danych osobowych, wprowadzona zarządzeniem Nr 31/2005 Prezydenta Miasta Świnoujście z dnia 31.01.2005 r. w sprawie wprowadzenia do użytku służbowego instrukcji zarządzania systemem informatycznym

służącym do przetwarzania danych osobowych w Urzędzie Miasta Świnoujście[29] oraz zarządzeniem Nr 569/06 z dnia 11.07.2006 r. w sprawie ustalenia „Polityki Bezpieczeństwa Informacji w zakresie przetwarzania danych osobowych w Urzędzie Miasta Świnoujście".

W 2014 r. Prezydent przygotował projekty dwóch procedur wewnętrznych w zakresie bezpieczeństwa systemów informatycznych: „Instrukcję zarządzania, eksploatacji i wdrażania Systemów Informatycznych w Urzędzie" oraz „Politykę Bezpieczeństwa w Urzędzie". Do dnia zakończenia przedmiotowej kontroli nie zostały one wdrożone.

(dowód: akta kontroli str. 337-364, 443-446)

Ustalone nieprawidłowości

W działalności kontrolowanej jednostki w przedstawionym wyżej zakresie stwierdzono następujące nieprawidłowości:

W Urzędzie nie wdrożono całościowej Polityki Bezpieczeństwa Informacji[30], która jest elementem systemu zarządzania bezpieczeństwem informacji w zakresie określonym w § 20 ust. 1, ust. 2 pkt 1 i ust. 3 rozporządzenia KRI. W 2006 r. opracowano PBI, która nie dotyczyła wszystkich danych jakie są przetwarzane w Urzędzie, lecz tylko danych osobowych.

(dowód: akta kontroli str. 337-364)

Przepis § 20 ust. 1 ww. rozporządzenia stanowi, 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 z uwzględnieniem takich atrybutów, jak autentyczność, rozliczalność, niezaprzeczalność i niezawodność.

§ 20 ust. 2 pkt 1 rozporządzenia KRI stanowi, że zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez zapewnienie przez kierownictwo podmiotu publicznego warunków umożliwiających realizację i egzekwowanie m.in. aktualizacji regulacji wewnętrznych w zakresie dotyczącym zmieniającego się otoczenia.

§ 20 ust. 3 rozporządzenia KRI stanowi, że wymagania w zakresie systemu zarządzania bezpieczeństwem informacji uznaje się za spełnione jeżeli została opracowana na podstawie Polskiej Normy: PN-ISO/IEC 27001, a ustanowienie zabezpieczeń, zarządzania ryzykiem oraz audytowanie odbywa się na podstawie Polskich Norm związanych z tą normą, w tym PN-ISO/IEC 17799 - w odniesieniu do ustanowienia zabezpieczeń. W pkt 5.1.1. normy PN-ISO/IEC17799 wskazano opracowanie i stosowanie dokumentu PBI.

Sekretarz Miasta wyjaśnił m.in: *Urząd przykłada dużą wagę do problemów, które są* wyszczególnione w rozporządzeniu KRI. Nie dokonano aktualizacji jeszcze obowiązującego *dokumentu, gdyż przystąpiono do starannego przygotowania nowej PBI własnymi siłami, mimo dużej ilości bieżących zadań. Jest to proces wymagający i czasochłonny...Obecnie trwają prace nad załącznikami do tego dokumentu, które będą w szczegółach odnosiły się do poszczególnych zagadnień bezpieczeństwa informacji. Jednym z załączników do PBI będzie „Instrukcja zarządzania systemem informatycznym w Urzędzie Miasta Świnoujście", w którym między innymi będą następujące informacje: szczegółowy wykaz pomieszczeń, w których dane są gromadzone i przetwarzane, ich usytuowanie oraz zabezpieczenie; aktualny schemat wewnętrznej struktury sieci teleinformatycznej, rozmieszczenia serwerów, na których zlokalizowane są bazy zawierające dane osobowe oraz opis zabezpieczeń systemowych; aktualny wykaz serwerów i komputerów stanowiskowych, na których znajdują się bazy danych zawierające dane osobowe oraz opis systemów operacyjnych i ich zabezpieczeń przed nieautoryzowanym dostępem; aktualny wykaz zbiorów, w których przetwarzane są dane osobowe wraz ze wskazaniem programów zastosowanych do ich przetwarzania.*

(dowód: akta kontroli str. 447-458)

[29] Zwane dalej „Instrukcją zarządzania systemem informatycznym".

[30] Zwana dalej „PBI".

2.2. Sprzęt Informatyczny

Opis stanu faktycznego

Na próbie 10 komputerów wykorzystywanych przez Urząd[31] oraz 5 komputerów przekazanych[32] Urzędowi do użytkowania przez MSWiA, ustalono że inwentaryzację zasobów informatycznych ujęto w układzie tradycyjnej książki inwentarzowej (dla potrzeb rachunkowości), która nie zawierała danych szczegółowych o konfiguracji technicznej urządzeń czy też o zainstalowanym oprogramowaniu.

(dowód: akta kontroli str. 245-256, 306-312)

W 2011 r. Urząd założył karty informacyjne dla zasobów informatycznych, w tym dla 3 z 15 objętych badaniem komputerów. Karty te zawierały jednak nieaktualne dane o oprogramowaniu zainstalowanym na danym urządzeniu (m.in. 2 karty zawierały dane o nieaktualnych poprawkach do systemu operacyjnego, a 3 karty – o nieaktualnym oprogramowaniu antywirusowym). Dla jednego badanego serwera nie sporządzono karty informacyjnej.

(dowód: akta kontroli str. 245-246, 257-305, 311-312)

Ustalone nieprawidłowości

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

Urząd dla 15 badanych komputerów i jednego serwera nie posiadał dokumentów z aktualną informacją o zainstalowanym na nich oprogramowaniu (np. informacji o aktualnym oprogramowaniu antywirusowym, poprawkach do systemu operacyjnego) oraz kompletnych danych o ich konfiguracji.

(dowód: akta kontroli str. 245-312)

Zgodnie z § 20 ust. 2 pkt 2 rozporządzenia KRI Urząd zobowiązany jest do zapewnienia przez kierownictwo podmiotu publicznego warunków umożliwiających realizację i egzekwowanie utrzymywania aktualności inwentaryzacji sprzętu i oprogramowania służącego do przetwarzania informacji obejmującej ich rodzaj i konfigurację.

Zgodnie z pkt 7.1.1 normy PN-ISO/IEC 17799:2007 wszystkie aktywa informatyczne powinny być zidentyfikowane i aktualizowane. Aktualna inwentaryzacja m.in. sprzętu informatycznego powinna także zawierać informację o jego rodzaju i konfiguracji, przez co możliwe będzie odtworzenie po katastrofie lub innym zdarzeniu losowym.

Sekretarz Miasta wyjaśnił: *Konfiguracja sprzętu i oprogramowania jest określana w dokumentach OT (przyjęcia środka trwałego). W najbliższym czasie, podczas przeprowadzania inwentaryzacji rocznej w Urzędzie zostanie przeprowadzona aktualizacja inwentaryzacji sprzętu i oprogramowania obejmująca ich rodzaj i konfigurację*.

(dowód: akta kontroli str. 447-458)

2.3. Analizy utraty integralności, poufności lub dostępności informacji

Opis stanu faktycznego

W związku z § 20 ust. 2 pkt 3 rozporządzenia KRI w Urzędzie prowadzono okresowe analizy utraty integralności, poufności i dostępności informacji. W Urzędzie przeprowadzono w dniu 29.08.2012 r. zewnętrzny audyt bezpieczeństwa systemów informatycznych. Przeprowadzony audyt badał zagrożenia atakiem zewnętrznym na publiczny adres IP. Badaniem objęto ewentualne usterki i błędy powodujące: możliwość zdalnego dostępu do zasobów; pozwalające na atak DoS (teoretycznie) – zablokowanie usług, serwisów, przerwy w działaniu; pozwalające na wyciek informacji. W wyniku przeprowadzonego audytu wykryto 7 zagrożeń, wynikających z używania nieaktualnego oprogramowania Apache/PHP.

(dowód: akta kontroli str. 191-199, 201-205)

[31] Tj. 4 komputerów wykorzystywanych w Wydziale Organizacyjnym, 4 - w Biurze Geodety Miasta, 1 - w Wydziale Komunikacji oraz 1 – w Wydziale Podatków i Opłat Lokalnych.

[32] Na podstawie porozumienia z 5 listopada 2010 r. (aneksowanego w dniu 31 grudnia 2013 r.).

Prezydent wyjaśnił m.in., że *aktualizacja oprogramowania skutecznie zniwelowała potencjalne ryzyko.*

(dowód: akta kontroli str. 198-199)

2.4. Zarządzanie uprawnieniami do pracy w systemach informatycznych

Opis stanu faktycznego

W Instrukcji zarządzania systemem informatycznym określono m.in. „Procedurę uwierzytelniania użytkownika w systemie informatycznym", „Procedurę rejestrowania/ wyrejestrowania użytkownika z systemu informatycznego", „Procedurę rozpoczęcia pracy w systemie informatycznym" oraz „Procedurę nadawania uprawnień do przetwarzania danych osobowych i rejestracji tych uprawnień w systemie informatycznym".

(dowód: akta kontroli str. 337-347)

Konta 5 z 10 badanych użytkowników systemu EOD eKancelaria, którzy zakończyli zatrudnienie w Urzędzie w badanym okresie, zostały zablokowane stosownie do wymogu określonego w § 20 ust. 2 pkt 4 rozporządzenia KRI oraz w pkt 2.3. Procedury rejestrowania/wyrejestrowania użytkownika z systemu informatycznego.

(dowód: akta kontroli str. 324-335)

Analizując uprawnienia 15 osób pracujących w systemach tzw. „dziedzinowych" ustalono, że 7 użytkowników posiadało uprawnienia do systemów w stopniu adekwatnym do realizowanych zadań (określonych w regulaminie organizacyjnym oraz w Karcie zakresu obowiązków, uprawnień i odpowiedzialności pracowników).

(dowód: akta kontroli str. 65, 367)

W toku kontroli ustalono, że wg stanu na 23.09.2014 r. użytkownicy 15 badanych komputerów, niebędący pracownikami służb informatycznych, posiadali uprawnienia administratora systemu na używanych przez nich komputerach, i mogli zainstalować program Microsoft Word Viwer. Użytkownik „Gość" został wyłączony na wszystkich badanych jednostkach komputerowych.

(dowód: akta kontroli str. 245-246, 311-312)

Ustalone nieprawidłowości

W działalności kontrolowanej jednostki w przedstawionym wyżej zakresie stwierdzono następujące nieprawidłowości:

1) Konta 4 z 10 użytkowników systemu eKancelaria zostały zablokowane w okresie od 3 do 8 miesięcy po zakończeniu zatrudnienia w Urzędzie. Ponadto konto jednego użytkownika nie zostało zablokowane[33], mimo zakończenia zatrudnienia w dniu 13.05.2014 r. Stanowiło to naruszenie § 20 ust. 2 pkt 4 i 5 rozporządzenia KRI oraz w pkt 2.3. Procedury rejestrowania/wyrejestrowania użytkownika z systemu informatycznego.

W żadnym z 10 badanych przypadków nie złożono wniosku o cofnięcie uprawnień do przetwarzania danych osobowych (wg wzoru stanowiącego załącznik nr 1 do Instrukcji zarządzania systemem informatycznym).

(dowód: akta kontroli str. 324-335, 470-471)

Przepisy § 20 ust. 2 pkt 4 i 5 rozporządzenia KRI stanowią, że zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez zapewnienie przez kierownictwo podmiotu publicznego warunków umożliwiających realizację i egzekwowanie m.in. działań zapewniających, że osoby zaangażowane w procesie 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. A w przypadku zmiany zadań ww. osób, bezzwłocznej zmiany przypisanych im uprawnień.

W pkt 2.3. Procedury rejestrowania/wyrejestrowania użytkownika z systemu informatycznego określono, że ustanie stosunku pracy powoduje wyrejestrowanie

[33] Według stanu na 23.09.2014 r.

użytkownika przez administratora systemu. O fakcie ustania stosunku pracy administrator systemu jest niezwłocznie informowany przez przełożonego.

(dowód: akta kontroli str. 337-347)

Sekretarz Miasta wyjaśnił m.in.: *Głównym systemem sieciowym w Urzędzie jest Novell® Open Enterprise Server. Po uzyskaniu informacji o odejściu pracownika jest natychmiast usuwany z systemu sieciowego (wszystkie wyżej wymienione osoby miały usunięte konta w systemie Novell) oraz zmieniany lub likwidowany jest jego profil z lokalnego komputera. Jest to najbardziej efektywna blokada użytkownika, gdyż od tego momentu nie może już korzystać z żadnej aplikacji Urzędu. Blokowanie zwalnianych użytkowników w aplikacjach jest już wtórne, choć konieczne. Wyżej wymienione osoby zostały zablokowane z opóźnieniem z chwilą otrzymania informacji o zwolnieniu oraz przez przeoczenie. Jeden użytkownik nie został zgłoszony przez przełożonego do administratora sieci i systemów, że został zwolniony.*

(dowód: akta kontroli str. 447-458)

2) Uprawnienia 8 z 15 badanych osób pracujących z systemami tzw. „dziedzinowymi" posiadało uprawnienia do systemów nieodpowiadające zakresowi zadań określonych w Karcie obowiązków, uprawnień i odpowiedzialności (tj. do systemów EOD eKancelaria i Geo-Info). Stanowiło to naruszenie § 20 ust. 2 pkt 4 rozporządzenia KRI.

(dowód: akta kontroli str. 9-10, 61-91, 367-395)

Sekretarz Miasta wyjaśnił m.in.: *Osoby posiadające nadane uprawnienia w systemie EOD eKancelaria oraz w systemie Geo-Info wykonują z racji pełnienia swoich obowiązków - jako kierownicy, są to: Zastępcy Prezydenta, Skarbnik, Sekretarz, Naczelnicy Wydziałów i Kierownicy Biur oraz jako pracownicy merytoryczni: inspektorzy. Ponadto informuję, że zgodnie z § 20 ust. 2 pkt 5 rozporządzenia KRI zakresy obowiązków zostaną uzupełnione.*

(dowód: akta kontroli str. 450-458, 463)

3) Objęci badaniem wszyscy użytkownicy systemów informatycznych (tj. 15 osób), niebędący pracownikami służb informatycznych, posiadali uprawnienia administratora systemu na używanych przez nich komputerach, w związku z czym mogli samodzielnie instalować dowolne oprogramowanie. Było to niezgodne z § 20 ust. 2 pkt 4 oraz pkt 7 lit. c rozporządzenia KRI. Ponadto, zgodnie z normą PN-ISO/IEC 27001, załącznik A, pkt A.11.2.2 oraz normą PN-ISO/IEC 17799:2007 pkt 11.2.2 lit. b należy ograniczać i kontrolować przyznawanie i korzystanie z przywilejów w systemach informatycznych, które winny być przyznawane według minimalnych wymagań wynikających z przydzielonych pracownikom zadań i tylko wtedy, gdy jest to konieczne.

(dowód: akta kontroli str. 245-246, 311-312)

Sekretarz Miasta wyjaśnił: *Wszystkie skontrolowane komputery posiadały użytkowników o uprawnieniach administracyjnych. Nie oznacza to, że komputery były bezpośrednio wystawione na ataki, gdyż na wszystkich stanowiskach jest wyłączone konto Gość i działa oprogramowanie antywirusowe ESET. Oprogramowanie antywirusowe ESET posiada centralny panel administracyjny automatycznie pobierający dane o stanie bezpieczeństwa komputerów lokalnych, ponadto umożliwia zdalne skanowanie dowolnego komputera w sieci lokalnej. Takie rozwiązanie umożliwia informatykom Urzędu bieżące monitorowanie ewentualnych zagrożeń. Chcąc wypełnić wymagania rozporządzenia KRI, wszystkie konta użytkowników zostaną pozbawione uprawnień administracyjnych z czasowym wyłączeniem przypadków, gdzie pozbawienie takich uprawnień uniemożliwi pracę na starszych aplikacjach.*

(dowód: akta kontroli str. 447-458)

2.5. Szkolenia pracowników przetwarzających informacje

Opis stanu faktycznego

W badanym okresie w Urzędzie nie planowano szkoleń dla pracowników zaangażowanych w proces przetwarzania informacji w zakresie zachowania bezpieczeństwa informacji. Według stanu na 31.05.2012 r. było zatrudnionych 224 pracowników na stanowiskach urzędniczych, a wg stanu na 31.08.2014 r. - 239.

(dowód: akta kontroli str. 396-397, 470-471, 481)

Jeden pracownik Urzędu (tj. Administrator Bezpieczeństwa Informacji[34]) uczestniczył w dwóch szkoleniach z zakresu przygotowania PBI oraz audytu wewnętrznego bezpieczeństwa informacji zgodnie z wytycznymi Ministra Finansów i MAiC na podstawie wymagań rozporządzenia KRI.

(dowód: akta kontroli str. 397)

W zakresie zadań ABI (z 14.03.2014 r.) określono, że jest on zobowiązany m.in. do prowadzenia szkoleń: wstępnego dla pracowników oraz okresowego dla poszczególnych wydziałów.

(dowód: akta kontroli str. 365-366)

Ustalone nieprawidłowości

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

W badanym okresie Urząd nie zapewnił szkoleń dla wszystkich użytkowników systemów informatycznych wykorzystywanych przez Urząd, w zakresie zachowania bezpieczeństwa informacji, co stanowiło naruszenie § 20 ust. 2 pkt 6 rozporządzenia KRI.

(dowód: akta kontroli str. 397, 479-485)

Przepis § 20 ust. 2 pkt 6 ww. rozporządzenia stanowi, że zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez zapewnienie przez kierownictwo podmiotu publicznego warunków umożliwiających realizację i egzekwowanie m.in. działań zapewniających szkolenie osób zaangażowanych w proces przetwarzania informacji, ze szczególnym uwzględnieniem takich zagadnień jak: zagrożenia bezpieczeństwa informacji, skutki naruszania zasad bezpieczeństwa informacji, stosowanie środków zapewniających bezpieczeństwo informacji.

Sekretarz Miasta wyjaśnił m.in.*: W dniu 21.04.2009 r. Administrator Danych Osobowych skierował pismo do wszystkich komórek organizacyjnych Urzędu w sprawie obowiązkowych szkoleń z zakresu ochrony danych osobowych, które odbyły się w maju 2009 r. Zostali przeszkoleni wszyscy pracownicy, którzy się zgłosili. Ponadto, szkolenia z ochrony danych osobowych prowadzone były w grudniu 2010 r. w ramach środków uzyskanych z Programu Operacyjnego Kapitał Ludzki. W bieżącym roku powołano ABI, któremu w zakresie obowiązków powierzono prowadzenie wstępnych i okresowych szkoleń dla pracowników.*

(dowód: akta kontroli str. 468-471, 482-485)

2.6. Procedury bezpiecznej pracy przy przetwarzaniu mobilnym i pracy na odległość

Opis stanu faktycznego

W Instrukcji zarządzania systemem informatycznym nie określono procedury gwarantującej bezpieczną pracę przy przetwarzaniu mobilnym i pracy na odległość.

(dowód: akta kontroli str. 337-347)

Ustalone nieprawidłowości

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

W badanym okresie w Urzędzie nie wprowadzono procedury gwarantującej bezpieczną pracę przy przetwarzaniu mobilnym i pracy na odległość, co stanowiło naruszenie § 20 ust. 2 pkt 8 rozporządzenia KRI.

[34] Zwany dalej „ABI"

(dowód: akta kontroli str. 337-347)

Przepis § 20 ust. 2 pkt 8 ww. rozporządzenia stanowi, że zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez zapewnienie przez kierownictwo podmiotu publicznego warunków umożliwiających realizację i egzekwowanie m.in. ustanowienia podstawowych zasad gwarantujących bezpieczną pracę przy przetwarzaniu mobilnym i pracy na odległość.

Sekretarz Miasta wyjaśnił, że *Procedura zgłaszania takich zdarzeń będzie elementem opracowywanych obecnie załączników do PBI.*

(dowód: akta kontroli str. 447-458)

2.7. Umowy serwisowe

Opis stanu faktycznego

W umowach na wdrożenie oraz serwisowanie jednego z 4 badanych systemów (tj. odpadywgminie.com.) zawarto zapis o zobowiązaniu wykonawcy do ochrony danych poufnych, a ich przetwarzanie zostało zastrzeżone w zakresie i celu związanym z realizacją umowy, stosownie do wymogu określonego w § 20 ust. 2 pkt 10 rozporządzenia KRI.

Wdrożenie i serwisowanie System FORIS dokonano bez zawarcia pisemnej umowy, na podstawie wewnętrznej procedury (tj. rozeznania rynku), określonej w regulaminie udzielania zamówień publicznych, których wartość nie przekracza 14 tys. euro. System ten został zainstalowany i był aktualizowany przez pracowników Urzędu (poprzez udostępnianie zaktualizowanych wersji na stronie producenta).

(dowód: akta kontroli str. 398-405, 419-426, 432-436, 458)

Ustalone nieprawidłowości

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

W umowie z dnia 2.01.2014 r. na serwisowanie programu EOD eKancelaria, w umowie z dnia 31.10.2012 r. na wdrożenie systemu EOD eKancelaria, w umowie z dnia 3.12.2013 r. na dostarczenie modułu Geo-Info 6 i.Adres oraz w umowie z dnia 16.01.2012 r. i z dnia 3.01.2013 r. na nadzór autorski nad systemem Geo-Info nie zobowiązano wykonawców do zachowania odpowiedniego poziomu bezpieczeństwa informacji, co stanowiło naruszenie § 20 ust. 2 pkt 10 rozporządzenia KRI.

(dowód: akta kontroli str. 406-418)

Przepis § 20 ust. 2 pkt 10 rozporządzenia KRI stanowi, że zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez zapewnienie przez kierownictwo podmiotu publicznego warunków umożliwiających realizację i egzekwowanie następujących działań, m.in. zawierania w umowach serwisowych podpisanych ze stronami trzecimi zapisów gwarantujących odpowiedni poziom bezpieczeństwa informacji.

Sekretarz Miasta wyjaśnił m.in.: *Dostawca oprogramowania EOD eKancelaria posiada wdrożony System Zarządzania Bezpieczeństwem Informacji, zgodny z normą ISO PN-ISO/IEC 27001:2007. W przypadku Geo-Info w ostatnim okresie była dokonywana tylko aktualizacja oprogramowania. Urząd nie przekazuje komputerów do serwisów zewnętrznych. Zakup sprzętu w roku 2014 obejmuje trzyletnią gwarancję producenta w miejscu użytkowania z klauzulą, że dyski pozostają u właściciela sprzętu. W przypadku wymiany sprzętu z powodu uszkodzenia lub jego nieprzydatności, wymontowywane są twarde dyski. Oddawany do utylizacji sprzęt jest pozbawiony pamięci dyskowej. Odrębnie dyski twarde poddawane są utylizacji przez rozmagnesowywanie przez wyspecjalizowaną firmę.*

(dowód: akta kontroli str. 447-458, 487)

W ocenie NIK brak zapisów zobowiązujących wykonawców do zachowania poufności informacji w związku z realizacją umów na serwisowanie oraz na wdrożenie systemów, zwiększa ryzyko bezprawnego wykorzystania informacji jakie wykonawca otrzymał w związku z realizacją zawartej umowy.

2.8. Zgłaszanie incydentów naruszania bezpieczeństwa informacji

Opis stanu faktycznego

W Instrukcji zarządzania systemem informatycznym określono Procedurę postępowania w sytuacjach naruszenia ochrony danych osobowych. W procedurze tej określono przykłady naruszenia zabezpieczeń systemu oraz nałożono na pracowników obowiązek niezwłocznego powiadomienia przełożonego oraz ABI w przypadku podejrzenia naruszenia zabezpieczenia systemu.

(dowód: akta kontroli str. 337-347)

Prezydent wyjaśnił, że w *Urzędzie nie wystąpiły przypadki zgłoszenia incydentów naruszenia bezpieczeństwa informacji.*

(dowód: akta kontroli str. 199)

Sekretarz Miasta wyjaśnił, że *Procedura zgłaszania takich zdarzeń będzie elementem opracowywanych obecnie załączników do PBI.*

(dowód: akta kontroli str. 447-458)

2.9. Audyt wewnętrzny z zakresu bezpieczeństwa informacji.

Opis stanu faktycznego

W badanym okresie w Urzędzie nie planowano i nie przeprowadzono audytu wewnętrznego w zakresie bezpieczeństwa informacji.

(dowód: akta kontroli str. 6-7, 26-31)

Ustalone nieprawidłowości

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

W okresie od 1.01.2013 r. do 30.08.2014 r. nie przeprowadzono okresowego audytu wewnętrznego w zakresie bezpieczeństwa informacji, co stanowiło naruszenie § 20 ust. 2 pkt 14 rozporządzenia KRI.

(dowód: akta kontroli str. 6-7, 26-31)

Przepis § 20 ust. 2 pkt 14 rozporządzenia KRI stanowi, że zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez zapewnienie przez kierownictwo podmiotu publicznego warunków umożliwiających realizację i egzekwowanie m.in. zapewnienia okresowego audytu wewnętrznego w zakresie bezpieczeństwa informacji, nie rzadziej niż raz w roku.

Sekretarz Miasta wyjaśnił m.in.: *Wymogi KRI spowodowały w Urzędzie przegląd posiadanych i stosowanych polityk i procedur. Po weryfikacji okazało się, że stosowane procedury wymagają dostosowania do obecnych wymagań KRI. Urząd skoncentrował się na opracowaniu nowej PBI. Można było zlecić takie opracowanie i audyt firmom zewnętrznym, lecz koszty z tym związane były zbyt duże dla budżetu na technologie informacyjne. Z kolei ilość zadań jakie na bieżąco musi wykonywać Biuro Technologii Informacyjnych jest bardzo duża, gdyż bezwzględnym priorytetem jest zapewnienie ciągłości funkcjonowania systemów informatycznych i wysokiej jakości usług. Efektem audytu musi być zwiększenie rzeczywistego zabezpieczenia informacji. Dlatego trwają zaawansowane prace nad końcowym opracowaniem załączników do PBI, aby po wdrożeniu PBI przeprowadzony audyt w istotny sposób pomógł zwiększać bezpieczeństwo informacji. W roku 2012 przeprowadzono audyt bezpieczeństwa pod kątem możliwości ataku z zewnątrz. Na lata 2013–2014 nie wpisano audytu wewnętrznego do zadań Wydziału Audytu Wewnętrznego i Kontroli.*

(dowód: akta kontroli str. 447-458)

2.10. Tworzenie i testowanie kopii zapasowych danych i oprogramowania aplikacyjnego

Opis stanu faktycznego

W Instrukcji zarządzania systemem informatycznym określono „Procedurę tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania."[35]

(dowód: akta kontroli str. 337-347)

Według stanu na 25.09.2013 r. w pomieszczeniach Biura Technologii Informacyjnych przechowywane były kopie zapasowe roczne: za 2009 r., 2010 r., 2012 r. i za 2013 r. oraz kopie tygodniowe z 2014 r. Kopie zapasowe były przechowywane w szafach biurowych znajdujących się w pomieszczeniu Biura Technologii Informacyjnych, poza miejscem ich wytwarzania.

(dowód: akta kontroli str. 437)

Uwagi dotyczące badanej działalności

Urząd nie przechowywał kopii dziennych jako kopii pełnych, a także nie tworzył kopii miesięcznych oraz ich nie przetrzymywał przez okres 5 lat, co było niezgodne z zasadami określonymi w Procedurze tworzenia kopii zapasowych.

Zgodnie z pkt 1 i 2 Procedury tworzenia kopii zapasowych, kopie zapasowe dzienne są kopiami pełnymi, a nośniki z kopiami zapasowymi są przechowywane w pomieszczeniach Stanowiska ds. Informatyki (wg obowiązującego regulaminu organizacyjnego - Biuro Technologii Informacyjnych) pod nadzorem ABI. W pkt 3 i 4 ww. Procedury określono, że na koniec każdego miesiąca Stanowisko ds. Informatyki tworzy kopię miesięczną na płytach kompaktowych, które są przechowywane przez okres 5 lat.

(dowód: akta kontroli str. 343, 437)

Sekretarz Miasta wyjaśnił m.in.: *W Urzędzie tworzone są codziennie zapasowe kopie danych. Tworzona jest zawsze całkowita kopia baz i plików na serwerach (nie jest to kopia przyrostowa). Tworzenie kopii odbywa się w serwerowni, taśmy zapisywane codziennie pozostają w bibliotece taśmowej, zapisane taśmy z kopii piątkowej przenoszone są do innego pomieszczenia i następnie tam przechowywane. Jest to bardzo racjonalne działanie, chroniące dane i budżet Urzędu. Każdego roku jest odnotowywany przyrost danych, które muszą podlegać archiwizacji. W 2007 r. zakupiono bibliotekę taśmową, gdyż archiwizowane dane trudno było zmieścić na rozsądnej ilości dysków DVD. Na przykład na taśmie rocznej z roku 2012 znajdują się wszystkie dane od roku 2007 do 2012 włącznie. Procedury tworzenia kopii bezpieczeństwa w PBI z 2005 r. były oparte na tworzeniu kopii na płytach DVD. W obecnej sytuacji miesięczne kopie miałyby sens, gdyby dane były usuwane, lub tworzona byłaby kopia przyrostowa. Na taśmach rocznych znajdują się dane archiwalne, od bieżących aż do 7 lat wstecz. Zakup biblioteki taśmowej, stał się koniecznością, gdyż archiwizowane dane nie mieściły się na racjonalnej ilości płyt kompaktowych (płyta DVD zawiera ok. 4 GB danych, pojedyncza taśma, z biblioteki taśmowej użytkowanej w Urzędzie - 800 GB). Procedura zawarta w zarządzeniu Nr 31/2005 nie została zaktualizowana po zakupie w 2007 r. biblioteki taśmowej. Nowa PBI będzie uwzględniała bezpieczeństwo danych zgodnie z wymaganiami rozporządzenia KRI jak i racjonalność kosztów.*

(dowód: akta kontroli str. 464-467)

2.11. Format danych udostępniany przez badane systemy informatyczne

Opis stanu faktycznego

We wszystkich badanych systemach zapis danych wyjściowych[36], po wygenerowaniu pliku, można było zapisać m.in. w formatach: pdf, rtf, XML, gml. Wszystkie 4 badane systemy wykorzystywane przez Urząd spełniły warunek określony w załączniku nr 2 do rozporządzenia KRI, o możliwości zapisywania danych w jednym z formatów wymienionych w tym załączniku, zgodnie z przepisem § 18 ust. 1 rozporządzenia KRI.

(dowód: akta kontroli str. 207-208, 219, 234, 238, 453)

[35] Zwana dalej „Procedurą tworzenia kopii zapasowych".

[36] Zapis danych jest dokonywany w celu udostępnienia go w określonym formacie.

Ocena cząstkowa

Najwyższa Izba Kontroli ocenie negatywnie działalność Urzędu w zakresie wdrażania systemu zarządzania bezpieczeństwem systemów informatycznych, ponieważ w badanym okresie miały miejsce przypadki naruszenia przepisów rozporządzenia KRI, w szczególności:

- nie wdrożono PBI w oparciu o normę PN-ISO/IEC 27001:2007;
- nie przeprowadzono inwentaryzacji sprzętu komputerowego, obejmującej ich rodzaj i konfigurację;
- nie przestrzegano procedury odbierania uprawnień użytkownikom systemu EOD eKancelaria;
- nie przeszkolono w zakresie zachowania bezpieczeństwa informacji wszystkich pracowników zaangażowanych w proces przetwarzania informacji;
- nie opracowano procedur gwarantujących bezpieczną pracę przy przetwarzaniu mobilnym i pracy na odległość;
- nie przeprowadzono okresowego audytu wewnętrznego w zakresie bezpieczeństwa informacji.

3. Dostosowanie sposobu prezentacji informacji przez systemy do potrzeb osób niepełnosprawnych

Opis stanu faktycznego

Strona internetowa Urzędu została przygotowana do potrzeb osób niedowidzących poprzez umieszczenie w lewym górnym rogu znaczników pozwalających na otwarcie strony w wysokim kontraście lub wersji tekstowej.

Weryfikacja zgodności strony Urzędu ze standardem WCAG 2.0[37] w zakresie zasady 4 – Kompatybilność, dokonana poprzez wykorzystanie narzędzi dostępnych na stronie internetowej http://iiqsaw.w3.org/css-validator/ wykazała 120 błędów i 79 ostrzeżeń. Weryfikacja strony www. Urzędu z wykorzystaniem narzędzi dostępnych na stronie internetowej http://validator.w3.org/ wykazała 3 ostrzeżenia oraz wykazała zgodność testu kodu z językiem HTML5.

Strona internetowa Urzędu nie dawała możliwości odsłuchania zapisu informacji i nie zawierała informacji o sposobie udostępniania obsługi dla osób doświadczających trwałej lub czasowej trudności w komunikowaniu się (m.in. o dostępności za pomocą innych komunikatorów internetowych).

Na stronie www. Urzędu umieszczono link do strony BIP Urzędu, która działa pod adresem http://bip.um.swinoujscie.pl/. W prawym górnym rogu znajdowała się zakładka „Wersja dla słabowidzących" - pozwalająca otworzyć stronę w wysokim kontraście oraz zapisaną większą czcionką.

(dowód: akta kontroli str. 239-244)

Ocena cząstkowa

Najwyższa Izba Kontroli nie formułuje oceny cząstkowej 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 dnia 30.05.2015 r.

IV. Wnioski

Przedstawiając powyższe oceny 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[38], wnosi o*:*

1) *Wdrożenie całościowej PBI określającej zasady bezpieczeństwa informacji, zgodnej z normą PN-ISO/IEC 27001.*
2) *Prowadzenie aktualnej i kompletnej inwentaryzacji sprzętu informatycznego, obejmującej jego rodzaj i konfigurację*.

[37] Web Content Accessibility Guidelines (tj. wytycznych dotyczących ułatwień dostępu do treści publikowanych w internecie).

[38] Dz. U. z 2012 r., poz. 82 ze zm., zwana dalej: „ustawą o NIK".

3) *Odebranie użytkownikom systemów informatycznych, niebędących pracownikami służb informatycznych, uprawnień umożliwiających instalowanie oprogramowania.*

4) *Przeszkolenie wszystkich osób zaangażowanych w proces przetwarzania informacji w zakresie zachowania bezpieczeństwa informacji.*

5) *Opracowanie i wdrożenie procedur gwarantujących bezpieczną pracę przy przetwarzaniu mobilnym i pracy na odległość.*

6) *Zawarcie w umowach serwisowych systemów EOD eKancelaria i Geo-Info zapisów gwarantujących odpowiedni poziom bezpieczeństwa informacji.*

7) *Wykonywanie okresowych audytów wewnętrznych w zakresie bezpieczeństwa informacji.*

8) *Dostosowanie Procedury tworzenia kopii zapasowych do wprowadzonych w Urzędzie rozwiązań technicznych dotyczących tworzenia kopii.*

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 ust. 1 i 2 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 Szczecinie.

Obowiązek poinformowania NIK o sposobie wykonania wniosków

Zgodnie z art. 62 ustawy o NIK proszę o poinformowanie Najwyższej Izby Kontroli, w terminie 21 dni od dnia otrzymania wystąpienia pokontrolnego, o sposobie wykonania wniosków 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.

Szczecin, dnia października 2014 r.

Najwyższa Izba Kontroli
Delegatura w Szczecinie

Kontroler
Bogumiła Mędrzak
Główny specjalista kontroli państwowej

....