NAJWYŻSZA IZBA KONTROLI
Departament Administracji Publicznej

KAP.410.002.05.2016
P/16/006

WYSTĄPIENIE POKONTROLNE

NAJWYŻSZA IZBA KONTROLI
ul. Filtrowa 57, 02-056 Warszawa
T +48 22 444 53 08, F +48 22 444 52 52
kap@nik.gov.pl
Adres korespondencyjny: Skr. poczt. P-14, 00-950 Warszawa 1

I. Dane identyfikacyjne kontroli

Numer i tytuł kontroli

P/16/006 – System Rejestrów Państwowych – bezpieczeństwo, funkcjonowanie i użyteczność

Jednostka przeprowadzająca kontrolę

Najwyższa Izba Kontroli
Departament Administracji Publicznej

Kontrolerzy

1. Agnieszka Klimowicz, główny specjalista kontroli państwowej, upoważnienie do kontroli nr KAP/2/2016 z dnia 31 maja 2016 r.
2. Bartosz Tajer, główny specjalista kontroli państwowej, upoważnienie do kontroli nr KAP/4/2016 z dnia 31 maja 2016 r.
3. Piotr Bielecki, specjalista kontroli państwowej, upoważnienie do kontroli nr KAP/5/2016 z dnia 31 maja 2016 r.

(dowód: akta kontroli str. 1-3)

Jednostka kontrolowana

Centralny Ośrodek Informatyki, ul. Suwak 3, 02-676 Warszawa

Kierownik jednostki kontrolowanej

Monika Jakubiak, Dyrektor Centralnego Ośrodka Informatyki od 1 września 2016 r. (wcześniej Rafał Leśkiewicz od 1 czerwca 2016 r. do 31 sierpnia 2016 r., Adam Sobczak od 27 stycznia 2016 r. do 31 maja 2016 r. i Nikodem Bończa Tomaszewski od 19 kwietnia 2012 r. do 25 stycznia 2016 r.)

(dowód: akta kontroli str. 1824-1831)

Okres objęty kontrolą

Od 1 stycznia 2013 r. do dnia zakończenia czynności kontrolnych w jednostce, tj. do 8 września 2016 r.

Wykaz skrótów i pojęć użytych w wystąpieniu:

- aplikacje wspierające – niezależne od Systemu Rejestrów Państwowych oprogramowanie wykorzystywane w Urzędach Stanu Cywilnego,
- BUSC – Baza Usług Stanu Cywilnego,
- COI – Centralny Ośrodek Informatyki,
- CRS – Centralny Rejestr Sprzeciwów,
- KN – Komponent Niejawny,
- MC – Ministerstwo Cyfryzacji,
- MSW – Ministerstwo Spraw Wewnętrznych,
- MSWiA – Ministerstwo Spraw Wewnętrznych i Administracji,
- PESEL – Powszechny Elektroniczny System Ewidencji Ludności,
- RDO – Rejestr Dowodów Osobistych,
- rozporządzenie KRI – rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów[1],
- sieć OST 112 – ogólnopolska sieć teleinformatyczna zapewniająca połączenie między infrastrukturą SRP zlokalizowaną w gminach a centralnym modułem SRP,

[1] Dz. U. z 2016 r. poz. 113.

- SOP – System Odznaczeń Państwowych,
- SRP – System Rejestrów Państwowych, wytworzony i uruchomiony na zlecenie MSW, od 2016 r. funkcjonowanie systemu nadzoruje Minister Cyfryzacji,
- umowa SLA – (ang. Service Level Agreement) umowa dotycząca poziomu usług informatycznych i ich parametrów,
- ustawa o dowodach osobistych – ustawa z dnia 6 sierpnia 2010 r. o dowodach osobistych[2],
- ustawa o ewidencji ludności – ustawa z dnia 24 września 2010 r. o ewidencji ludności[3],
- ustawa Prawo o aktach stanu cywilnego – ustawa z dnia 28 listopada 2014 r. Prawo o aktach stanu cywilnego[4],
- walidacja danych – sprawdzanie prawidłowości danych wprowadzanych do systemu,
- właściciel systemu – do 31 grudnia 2015 r. minister właściwy do spraw wewnętrznych, od 1 stycznia 2016 r. minister właściwy do spraw informatyzacji,
- Źródło – aplikacja umożliwiająca korzystanie z Systemu Rejestrów Państwowych.

II. Ocena kontrolowanej działalności

Ocena ogólna

Centralny Ośrodek Informatyki wywiązał się z powierzonego przez Ministerstwo Spraw Wewnętrznych zadania budowy Systemu Rejestrów Państwowych, jednak jego uruchomienie nastąpiło z dwumiesięcznym opóźnieniem, a po udostępnieniu systemu ujawniło się w jego działaniu wiele błędów i braków w funkcjonalnościach (zwłaszcza w pierwszych trzech miesiącach działania). Utrudniło to sprawną realizację zadań przez użytkowników SRP. W ocenie NIK, opóźnienie w uruchomieniu SRP i błędy w jego działaniu wynikały z przyczyn leżących zarówno po stronie zlecającego budowę systemu – MSW, jak i wykonawcy – COI, w szczególności z:

- zbyt krótkiego czasu na realizację projektu, co niekorzystnie wpłynęło na jakość udostępnionego systemu;
- braku skutecznego, konsekwentnego stosowania metodyk zarządzania projektami (m.in. przedstawiciele MSW nie brali udziału w części spotkań w COI dotyczących wytwarzania oprogramowania SRP przy zastosowaniu metodyki *Scrum*[5]);
- braku decyzji MSW o przeprowadzeniu przez COI wdrożenia pilotażowego, które pozwoliłoby na przetestowanie systemu w praktyce oraz wykrycie i usunięcie wad;
- zgłaszania przez użytkowników dodatkowych wymagań co do funkcjonalności SRP w trakcie testów oprogramowania;
- błędów w oprogramowaniu opracowanym przez COI, w związku z czym SRP został odebrany i uruchomiony warunkowo po upływie dwóch miesięcy od pierwotnie planowanego terminu;
- równolegle prowadzonych prac nad aktami prawnymi z zakresu rejestracji stanu cywilnego i prac programistycznych przy budowie SRP.

---

2 Dz. U. z 2016 r. poz. 391, ze zm.
3 Dz. U. z 2016 r. poz. 722, ze zm.
4 Dz. U. poz. 1741, ze zm.
5 *Scrum* – metodyka prowadzenia projektów, która zakłada podział prac na mniejsze etapy i umożliwia elastyczne reagowanie na uwagi uczestników projektu.

COI podejmował działania w celu usuwania błędów i usterek w systemie oraz udzielał wsparcia technicznego użytkownikom SRP, jednakże rozwiązywanie zgłaszanych przez użytkowników problemów technicznych było wydłużone, szczególnie w pierwszych miesiącach po udostępnieniu systemu. Należy przy tym wskazać, że długi czas obsługi części zgłoszeń użytkowników wynikał z faktu, iż wymagane były rozstrzygnięcia o charakterze prawnym, leżące w gestii właściciela systemu (pierwotnie MSW, obecnie MC).

Ponadto, COI podjął działania zmierzające do zapewnienia rozwoju SRP, występując do MSW z propozycją przeznaczenia części zysku COI na działania rozwojowe oraz opracowując projekt ramowej umowy rozwojowej.

Zdaniem NIK, migracja danych do modułów PESEL i RDO w SRP była przeprowadzona należycie, z wykorzystaniem właściwych mechanizmów walidacji danych. Migracja danych o aktach stanu cywilnego do BUSC w SRP, zgromadzonych dotychczas w postaci elektronicznej nie była przedmiotem umowy z MSW, w ramach której wytworzono SRP.

COI podejmował działania w celu zapewnienia bezpieczeństwa SRP w powierzonym mu zakresie, a przyjęte rozwiązania były adekwatne do potrzeb i spełniały swoją funkcję. Zdaniem NIK, wprowadzona w COI z dniem 26 października 2015 r. *Polityka Bezpieczeństwa Informacji*, spełnia obowiązujące standardy w zakresie zarządzania bezpieczeństwem informacji.

W trakcie kontroli stwierdzono nieprawidłowość polegającą na nieodebraniu uprawnień dostępu do bazy danych SRP dwóm byłym pracownikom COI, co było niezgodne z § 20 ust. 2 pkt 5 rozporządzenia KRI; nieprawidłowość została usunięta w trakcie kontroli.

III. Opis ustalonego stanu faktycznego

Podstawowe informacje dotyczące obszaru objętego kontrolą

Integracja rejestrów państwowych w systemie informatycznym była jednym z celów przedsięwzięcia *pl.ID – polska ID karta* dofinansowanego z Unii Europejskiej ramach *Programu Operacyjnego Innowacyjna Gospodarka 2007-2013*, 7. Priorytet – *Społeczeństwo informacyjne – budowa elektronicznej administracji*, działanie 7.1 *Społeczeństwo informacyjne – budowa elektronicznej administracji*. W latach 2009-2012 za jego realizację było odpowiedzialne Centrum Projektów Informatycznych. W 2012 r., w związku ze zidentyfikowaniem istotnych problemów dotyczących założeń, przyjętej sekwencji prac i możliwości osiągnięcia zakładanych rezultatów, zmodyfikowano zakres przedsięwzięcia skupiając prace na stworzeniu jednolitego i spójnego systemu rejestrów państwowych. Od 2013 r. przygotowanie i wdrożenie Systemu Rejestrów Państwowych było realizowane w ramach zarządzanego przez Ministra Spraw Wewnętrznych programu *pl.ID*[6]. W umowie nr 4/DSiA/2013 z 25 lutego 2013 r. Minister Spraw Wewnętrznych powierzył zadania z tego zakresu Centralnemu Ośrodkowi Informatyki.

[6] Program *pl.ID* – projekt informatyczny, którego celem jest budowa rozwiązań technicznych mających poprawić jakość usług publicznych świadczonych przez państwo dla obywateli. W ramach tego programu realizowano szereg różnych projektów informatycznych.

Z dniem 16 listopada 2015 r. MSW zostało przekształcone w MSWiA[7] i nadzór nad COI objął Minister Spraw Wewnętrznych i Administracji. Od 1 stycznia 2016 r. funkcję organu nadzorującego COI przejął Minister Cyfryzacji[8].

W trakcie kontroli, na podstawie art. 29 ust. 1 pkt 2 lit. f ustawy z dnia 23 grudnia 1994 r. o Najwyższej Izbie Kontroli[9], uzyskano dodatkowe informacje od Ministra Cyfryzacji Pani Anny Streżyńskiej oraz Podsekretarza Stanu w MSWiA Pana Tomasza Zdzikota. Minister Cyfryzacji poinformowała, że posiadane przez MC informacje w przeważającej mierze zostały pozyskane w związku z włączeniem w strukturę MC części departamentów realizujących zadania z zakresu SRP w ramach MSW i MSWiA.

1. Udostępnienie Systemu Rejestrów Państwowych

1.1. Wydatki na przygotowanie, uruchomienie i udostępnienie SRP

Opis stanu faktycznego

System Rejestrów Państwowych był przygotowywany przez COI w latach 2013-2015, w oparciu o kolejne zlecenia Ministra Spraw Wewnętrznych, udzielane na podstawie ramowej umowy nr 4/DSiA/2013. COI realizował w szczególności zadania: budowy nowych i modernizacji istniejących rejestrów państwowych, optymalizacji aplikacji dostępowej, budowy komponentu niejawnego Systemu Rejestrów Państwowych, modernizacji serwerowni, dostarczenia i instalacji infrastruktury informatycznej dla dwóch ośrodków przetwarzania danych oraz na potrzeby funkcjonującego w ramach SRP komponentu niejawnego.

Maksymalne wynagrodzenie COI z tytułu realizacji umowy nr 4/DSiA/2013 ustalono w wysokości 121 623,5 tys. zł. Kwota ta, na podstawie aneksu do ww. umowy[10], wyniosła 109 000,0 tys. zł.

(dowód: akta kontroli str. 34-117, 215-292, 1583-1584, 1707-1708, 1719-1720, 1843-1907, 2772-2785, 3835-3837, 3843-3847, 3865-3870, 4327-4328, 4352-4355, 4533-4534, 4548-4556)

1.2. Wydatki na utrzymanie SRP

Opis stanu faktycznego

W latach 2015 i 2016 r. zadania w zakresie utrzymania SRP realizowane były przez COI na podstawie pięciu umów zawartych z MSW, MSWiA i MC[11]. Zakres umów obejmował świadczenie usług zapewniających poprawne i nieprzerwane funkcjonowanie SRP, tj.:

- utrzymanie właściwego poziomu jakościowego usług dla użytkowników m.in.: poprzez zarządzanie incydentami (w tym prowadzenie Service Desk), problemami, zmianą, poziomem usług, konfiguracją, dostępnością i pojemnością (zasobami), bezpieczeństwem, ciągłością działania, wiedzą, a także serwis oprogramowania, komunikację i szkolenia;

---

7 Na podstawie rozporządzenia Rady Ministrów z dnia 20 listopada 2015 r. w sprawie utworzenia Ministerstwa Spraw Wewnętrznych i Administracji (Dz. U. poz. 1946), które weszło w życie z dniem 24 listopada 2015 r., z mocą od 16 listopada 2015 r.

8 Na podstawie art. 42 ustawy z dnia 22 grudnia 2015 r. o zmianie ustawy o działach administracji rządowej oraz niektórych innych ustaw (Dz. U. poz. 2281).

9 Dz. U. z 2015 r. poz. 1096 oraz z 2016 r. poz. 677.

10 Aneks nr 3 do umowy nr 4/DSiA/2013 z 28 lutego 2015 r.

11 Umowy: 1/U/COI/MSW/2015 z 28 lutego 2015 r., zawarta pomiędzy MSW i COI, 3/DT/4.13/2015 (5/U/COI/MSW/2015) z 29 maja 2015 r., zawarta pomiędzy MSW i COI, 4/DT/4.13/2015/bp (4/U/COI/MSW/2015) z 29 maja 2015 r., zawarta pomiędzy MSW i COI, 11/DT/4.13/2015 (12/U/COI/MSW/2015) z 22 grudnia 2015 r., zawarta pomiędzy MSWiA i COI, 2/DIT/U/COI/2016 z 30 czerwca 2016 r., zawarta pomiędzy MC i COI.

- świadczenie usług dodatkowych, m.in.: modyfikacje, zmiany oprogramowania, rozwój aplikacji wspomagających eksploatację, utrzymanie i zarządzanie systemem, prowadzenie działań konsultacyjnych, eksperckich i analitycznych.

Wynagrodzenie COI z tytułu utrzymania SRP w okresie od 1 marca 2015 r. do 30 czerwca 2019 r. określono w łącznej wysokości 96 933,9 tys. zł. Według stanu na 31 maja 2016 r. na utrzymanie SRP wydatkowano łącznie 20 399,7 tys. zł. Kwota ta stanowiła 21% kwoty zaplanowanej na realizację zadań w zakresie utrzymania SRP.

(dowód: akta kontroli str. 2312-2315, 2683, 2726-2732, 3489-3669, 3835-3839, 3843-3847, 3865-3870, 3873, 3878, 4332, 4850)

1.3. Wydatki na rozwój SRP

Opis stanu faktycznego

W ustawie budżetowej na 2015 r. MSW nie zaplanowało środków na rozwój SRP przez COI. W ramach prac nad ustawą budżetową na 2016 r. MSW wnioskowało o zabezpieczenie środków na ten cel, jednak ostatecznie nie zostały one przyznane. Jak wyjaśnił Dyrektor COI Pan Rafał Leśkiewicz, począwszy od 2014 r. przedstawiciele COI sygnalizowali MSW potrzebę rozwoju i modernizacji SRP. W związku z powyższym COI m.in. wystąpił do Ministra Spraw Wewnętrznych z propozycją podziału wypracowanego zysku COI i przeznaczenia jego części na rozwój SRP oraz opracował i przekazał do MSW projekt ramowej umowy rozwojowej. MSW podjęło działania w celu oceny możliwości podziału zysku według propozycji COI, jednak ostatecznie środki te zwiększyły fundusz COI.

W dniu 29 czerwca 2016 r., w wyniku uzgodnień pomiędzy MC i COI, została zawarta umowa na rozwój SRP na okres czterech lat, na łączną kwotę nie przekraczającą 27 293,3 tys. zł.

(dowód: akta kontroli str. 2193-2194, 2197-2200, 2211-2311, 2577-2678, 3670-3762, 4333, 4619-4620)

1.4. Zarządzanie programem *pl.ID* w zakresie dotyczącym SRP

Opis stanu faktycznego

Program[12] *pl.ID* był zarządzany przez MSW w oparciu o metodykę MSP[13] oraz metodykę PRINCE2[14]. W ramach realizacji programu wyodrębniono pięć projektów, tj.: *System Rejestrów Państwowych*, *Rejestr Dowodów Osobistych*, *Rejestracja Stanu Cywilnego*, *Legalizacja* i *Serwerownia*. Struktury zarządzania programem i projektami zostały określone w zarządzeniach Ministra Spraw Wewnętrznych[15].

W związku z realizacją programu *pl.ID* Minister Spraw Wewnętrznych powołał m.in. Radę programu, będącą ciałem doradczym, w której mogli uczestniczyć, na zaproszenie przewodniczącego Rady, przedstawiciele COI jako wykonawcy SRP. Przedstawiciele COI uczestniczyli w posiedzeniach Rady w charakterze obserwatora i przysługiwał im jedynie głos doradczy, w związku z czym nie mieli oni realnego wpływu na decyzje podejmowane przez Radę. W okresie realizacji umowy nr 4/DSiA/2013, tj. od 25 lutego 2013 r. do 31 grudnia 2015 r., odbyło się jedynie sześć posiedzeń Rady programu. Za koordynację prac kierowników poszczególnych projektów, koordynację realizacji umowy i współpracę z COI odpowiadał

---

12 Zbiór wspólnie zarządzanych i koordynowanych projektów służących osiągnięciu wspólnego celu.

13 Ang. *Managing Successful Programmes.*

14 Ang. *Projects in Controlled Environment.*

15 Zarządzenie Nr 43 Ministra Spraw Wewnętrznych z dnia 15 maja 2013 r. w sprawie ustalenia struktury zarządzania projektem „pl.ID" (Dz. Urz. MSW poz. 43), zmienione Zarządzeniem Nr 2 Ministra Spraw Wewnętrznych z dnia 22 stycznia 2014 r. (Dz. Urz. MSW poz. 4) i Zarządzeniem Nr 21 Ministra Spraw Wewnętrznych z dnia 12 czerwca 2014 r. (Dz. Urz. MSW poz. 39).

powoływany przez MSW kierownik programu. W trakcie realizacji programu *pl.ID* aż siedmiokrotnie nastąpiła zmiana na tym stanowisku.

Na poziomie projektów wyodrębnionych w ramach programu *pl.ID* w skład struktur zarządczych wchodzili kierownicy komórek organizacyjnych MSW oraz Centrum Personalizacji Dokumentów[16], kierownicy projektów i zespoły projektowe. W strukturach tych nie zostały utworzone Komitety Sterujące, które zgodnie z metodyką PRINCE2 odpowiadają za ogólne ukierunkowanie i zarządzanie strategiczne projektem. Realizując projekty MSW nie stosowało całościowo rozwiązań oferowanych przez metodykę PRINCE2, a jedynie wykorzystywało jej elementy, m.in.: opracowywano i prowadzono analizy ryzyka, rejestr ryzyka, harmonogram, odbiory produktów (zleceń), raporty okresowe. Prowadząc harmonogram projektów MSW nie korzystało z narzędzi kontroli postępu prac, jakim są tzw. etapy zarządcze[17]. Pominięto zarządzanie jakością, domyślnie pozostawiając te kwestie wykonawcy (COI).

W umowie nr 4/DSiA/2013 nie zostały określone przez MSW wymagania odnośnie stosowania przez COI konkretnej metodyki zarządczej. W prace dotyczące budowy SRP zostali zaangażowani pracownicy różnych pionów COI[18]. Ponadto, zostały powołane zespoły odpowiedzialne m.in. za obsługę zarządczą oraz koordynację i wsparcie zadań związanych z wdrożeniem i uruchomieniem SRP.

W procesie zarządzania wytwarzaniem oprogramowania na potrzeby SRP, COI wykorzystywał metodykę *Scrum*. Zgodnie z wyjaśnieniami Dyrektora COI Pana Rafała Leśkiewicza, metodyka ta pozwalała na dostosowanie się do narzuconych ram czasowych projektu, skoncentrowanie na istocie wytwarzanego oprogramowania i znanych wymaganiach klienta, ponieważ zakres projektu wielokrotnie ulegał zwiększeniu, bądź zmianom. Pozwalała także na utrzymanie motywacji zespołu projektowego. Zastosowanie metodyki *Scrum* przewidziano również do obsługi prac w ramach gwarancji wynikającej z umowy nr 4/DSiA/2013. Dyrektor COI wyjaśnił także, że w procesie wytwarzania oprogramowania wykorzystywano wiele uznanych technik i metod wytwarzania[19] oraz zarządzania jakością kodu źródłowego[20].

Zgodnie z wyjaśnieniami Dyrektor COI Pani Moniki Jakubiak, po początkowym okresie współpracy MSW zrezygnowało z udziału w tych spotkaniach *Scrumowych*; wymagania MSW były przekazywane podczas innych spotkań, tj. analitycznych, prezentacyjnych, organizacyjnych.

(dowód: akta kontroli str. 121-132, 1281-1283, 1908-1914, 2736-2758, 2875-2876, 2880-2882, 3795-3796, 3838, 4350-4351, 4583-4618, 4656-4658, 4684-4685, 4693-4694, 4712-4718, 4732-4734)

1.5. Udostępnienie elementów/funkcjonalności SRP

Opis stanu faktycznego

Pierwotna data uruchomienia SRP, tj. 1 stycznia 2015 r., wynikała z przepisów ustawy Prawo o aktach stanu cywilnego oraz zmian do ustaw o ewidencji ludności

[16] Centrum Personalizacji Dokumentów jest jednostką budżetową nadzorowaną przez Ministra Spraw Wewnętrznych i Administracji. Realizuje zadania Ministra Spraw Wewnętrznych i Administracji w zakresie wydawania dokumentów dla obywateli polskich, pracowników administracji publicznej, funkcjonariuszy służb podległych Ministrowi Spraw Wewnętrznych i Administracji, cudzoziemców oraz udostępniania danych z rejestru PESEL.

[17] Część projektu, którą Kierownik projektu zarządza w imieniu Komitetu Sterującego w danym czasie. Po jej zakończeniu Komitet Sterujący dokonuje przeglądu dotychczasowych postępów, stanu realizacji Planu projektu, Uzasadnienia Biznesowego oraz ryzyk, a także Planu (następnego) Etapu, w celu podjęcia decyzji, czy projekt należy kontynuować. Źródło: OGC: *Managing Successful Projects with PRINCE2* (2009 ed.), TSO, ISBN 978-0-11-331059-3.

[18] Piony: ds. Kluczowych Projektów, Eksploatacji Systemów, Rozwoju Systemów, Rozwoju Produktów i Usług.

[19] Np. *Continuous Integration, Test Driven Development, Domain Driven Development*.

[20] Np. *pull request*, testy pokrycia.

i o dowodach osobistych. W grudniu 2014 r. został przesunięty przez MSW na 1 marca 2015 r. termin wejścia w życie ww. ustaw i uruchomienia SRP, co MSW uzasadniało brakiem gotowości systemu do wdrożenia, m.in. ze względu na zgłaszane przez użytkowników w trakcie testów akceptacyjnych usterki w wytworzonym przez COI oprogramowaniu. Pomimo, że COI zrealizował większość zleconych prac w wyznaczonych przez MSW terminach, do 1 stycznia 2015 r. nie zostały odebrane przez MSW zlecenia dotyczące prac COI w zakresie kluczowych rejestrów, tj. BUSC, PESEL, RDO, SOP, a także KN, aplikacji „Źródło" i dedykowanej dla MSW platformy e-usług. W związku z decyzją MSW o uruchomieniu systemu 1 marca 2015 r., na podstawie aneksu nr 3 do umowy nr 4/DSiA/2013 z 28 lutego 2015 r. MSW przesunęło na 28 lutego 2015 r. terminy realizacji zleceń dotyczących ww. elementów SRP, a następnie odebrało jedynie warunkowo od COI prace w tym zakresie, ze względu na stwierdzone problemy i błędy, które jednak nie miały charakteru krytycznego.

Kierownicy poszczególnych projektów w MSW prowadzonych w ramach programu *pl.ID*, wśród problemów zaistniałych w trakcie realizacji SRP wskazali[21] m.in.:

- liczne usterki w oprogramowaniu COI zidentyfikowane przez użytkowników podczas testów akceptacyjnych,
- brak realizacji przez COI części wymagań funkcjonalnych i niefunkcjonalnych wynikających z projektów technicznych,
- problemy we współpracy komponentów systemu,
- zgłaszanie przez użytkowników dodatkowych wymagań co do funkcjonalności w trakcie testów oprogramowania,
- brak opracowania ostatecznych zapisów ustawy Prawo o aktach stanu cywilnego i aktów wykonawczych do ustawy, uniemożliwiający dokładne określenie wymagań dla rejestracji stanu cywilnego.

SRP został uruchomiony z dniem 1 marca 2015 r., jednak na ten dzień nadal występowały w nim liczne usterki. Do momentu uruchomienia systemu nie zostały również wdrożone zalecenia wynikające ze zleconej przez MSW w grudniu 2014 r. ekspertyzy dotyczącej spełniania przez SRP wymogów funkcjonalnych i wydajnościowych oraz systemu zarządzania zmianą, ryzykiem i ciągłością działania po stronie COI. W raporcie z tej ekspertyzy został przedstawiony wykaz 10 obserwacji (spostrzeżeń usterek i nieprawidłowości lub uwag) wskazujących na zasadnicze problemy, których nierozwiązanie mogło spowodować poważne trudności w eksploatacji SRP i znacząco obniżać jakość systemu. Dyrektor COI Pan Rafał Leśkiewicz wyjaśnił m.in., że rekomendacje przedstawione w raporcie nie mogły być wzięte przez COI pod uwagę, ze względu na przekazanie tego raportu przez MSW do COI po raz pierwszy w styczniu 2016 r. Podał także, że raport opierał się jedynie na dokumentacji, której najpóźniejszy dokument jest datowany na 15 grudnia 2014 r. i większość rekomendacji należało uznać za nieaktualne, a część za niezasadne.

Po uruchomieniu SRP 1 marca 2015 r. COI sukcesywnie wprowadzał poprawki do systemu w oparciu o zestawione w tzw. „raportach rozbieżności" błędy i braki.

Ostateczny odbiór prac COI wynikających z umowy nr 4/DSiA/2013 nastąpił 31 grudnia 2015 r. Minister Cyfryzacji Pani Anna Streżyńska poinformowała, że przyjęty przez MSW termin realizacji SRP wynikał przede wszystkim z faktu, że był on finansowany z wykorzystaniem dofinansowania UE na lata 2007-2013, w związku z czym okres kwalifikowalności dla wydatków związanych z realizacją systemu upływał z dniem 31 grudnia 2015 r.

[21] W raportach końcowych dla poszczególnych projektów w ramach programu *pl.ID*.

Z wyjaśnień Dyrektor COI Pani Moniki Jakubiak wynika, że do momentu uruchomienia SRP zakres prac projektowych był rozszerzany przez MSW, wprowadzane były zmiany w wymaganiach, np. zmiany wynikające z faktu, że przepisy dotyczące prawa o aktach stanu cywilnego były tworzone równolegle z powstającym oprogramowaniem. W ocenie Kierownika Projektu w COI Pana Tomasza Ptaszyńskiego, zakres wymagań dla Bazy Usług Stanu Cywilnego został zwiększony o około 2/3 w stosunku do pierwotnych założeń. Ponadto, według wyjaśnień Dyrektora COI Pana Rafała Leśkiewicza, dotyczących realizacji napraw wynikających z raportów rozbieżności, *(…) W trakcie realizacji zmian MSW zgłosiło oczekiwania dotyczące wdrożenia innych zmian niż wskazano w Raportach Rozbieżności z 28 lutego 2015 r. W związku z tym sporządzając Protokoły Odbioru Produktu (…) dokonano aktualizacji Raportów Rozbieżności (…).*

Przed uruchomieniem SRP nie zostało przeprowadzone przez COI wdrożenie pilotażowe tego systemu. Działania takiego MSW nie przewidziało w harmonogramie programu *pl.ID*, jednak w grudniu 2014 r., po podjęciu przez MSW decyzji o przesunięciu wdrożenia SRP z 1 stycznia 2015 r. na 1 marca 2015 r. pojawiła się sugestia MSW przeprowadzenia takiego wdrożenia w ograniczonej liczbie gmin. Ostatecznie w styczniu 2015 r. MSW podjęło decyzję o przeprowadzeniu we wszystkich gminach, przy udziale COI, weryfikacji poprawności połączenia z SRP za pośrednictwem dedykowanej sieci teleinformatycznej OST 112 oraz uwierzytelnień użytkowników i aktualności certyfikatów. Według wyjaśnień Dyrektor COI Pani Moniki Jakubiak, działania te nie miały waloru wdrożenia pilotażowego SRP, ponieważ użytkownicy końcowi nie podejmowali faktycznej pracy na rzeczywistych danych i nie wykonywali formalnych czynności urzędowych w systemie.

(dowód: akta kontroli str. 564-573, 583-615, 670-716, 748-754, 1060-1064, 1069-1115, 1160-1257, 2071-2184, 2881-2889, 3796-3798, 3872-3873, 3876, 4532-4536, 4684-4685, 4693-4694, 4720-4725)

1.6. Problemy z funkcjonowaniem SRP po jego uruchomieniu 1 marca 2015 r.

Opis stanu faktycznego

Na podstawie badania próby losowo wybranych 3,0 tys. zgłoszeń użytkowników SRP zarejestrowanych w prowadzonym przez COI systemie ITSM *Atmosfera*, stanowiących 7,5% wszystkich zgłoszeń zarejestrowanych w okresie od 1 marca 2015 r. do 15 czerwca 2016 r., ustalono, że najczęściej powtarzającymi się problemami związanymi z funkcjonowaniem SRP były:

- błędy systemu w trakcie wykonywania różnych działań (np. komunikat o błędzie technicznym 500);
- problemy dotyczące dostępu do aplikacji „Źródło" (np. błędna konfiguracja stacji roboczych, w szczególności konfiguracja certyfikatów);
- problemy wynikające z braku migracji aktów stanu cywilnego do Bazy Usług Stanu Cywilnego;
- problemy z wykonywaniem działań ze względu na braki danych w rejestrze;
- awarie łącza teleinformatycznego wykorzystywanego na potrzeby SRP (problem z połączeniem się lub z komunikacją z SRP poprzez aplikację „Źródło");
- problemy z dostępnością systemu (przedłużające się prace modernizacyjne i problemy będące następstwem wprowadzenia aktualizacji);
- problemy z wykonywaniem czynności wskutek braku spójności danych (np. różne daty wydania/odbioru tego samego dokumentu w rejestrach);
- problemy z wykonywaniem czynności ze względu na nieintuicyjną obsługę systemu;

- problemy związane ze sprzętem (np. nieprawidłowe działanie skanera);
- powolne działanie systemu (tzw. problemy wydajnościowe).

Jak wyjaśnił Dyrektor COI Pan Rafał Leśkiewicz, do 17 czerwca 2016 r. w ramach gwarancji w COI zostało rozwiązanych i zamkniętych 15,3 tys. zgłoszeń użytkowników, zarejestrowanych w systemie ITSM *Atmosfera*.

W celu eliminacji pojawiających się po uruchomieniu SRP problemów COI realizowało prace naprawcze w ramach gwarancji do umowy nr 4/DSiA/2013. MC uzgodniło z COI wykonanie 180 poprawek w ramach gwarancji, w tym zmiany dotyczące ergonomii pracy w systemie oraz integrację pomiędzy rejestrami wchodzącymi w skład SRP. Jak wyjaśniła Dyrektor COI Pani Monika Jakubiak, ograniczenia czasowe uniemożliwiły realizację w ramach BUSC narzędzi umożliwiających sprawną i skuteczną migrację danych z aktów stanu cywilnego. W aplikacji „Źródło" przewidziano jedynie funkcję migracji pojedynczych aktów stanu cywilnego z aplikacji wspierających wykorzystywanych w gminach. COI zobowiązał się do przygotowania narzędzia wspierającego proces masowej migracji.

(dowód: akta kontroli str. 85, 1569-1579, 1977-2070, 1587-1588, 2316-2341, 2381-2569, 2786-2787, 3777-3801, 3824-3834, 3836-3837, 3839-3844, 3860-3864, 3872-4316, 4321-4345, 4527-4571, 4672-4676, 4683-4684, 4688-4689, 4692-4693, 4704-4876)

1.7. Prace związane z rozwojem oprogramowania SRP

Opis stanu faktycznego

Od momentu uruchomienia SRP, COI współpracował w trybie roboczym z MSW w zakresie prac rozwojowych. Jak wyjaśnił Dyrektor COI Pan Rafał Leśkiewicz, brak było formalnego zlecenia tego typu prac, a COI obsługiwał jedynie zgłoszenia mieszczące się w ramach gwarancji umownej. W 2015 r. w wyniku współpracy COI i MSW zostało zdefiniowanych ponad 220 zagadnień stanowiących rozszerzenia i ulepszenia funkcji SRP. W 2015 r. zostało również zorganizowane przez MSW spotkanie z przedstawicielami jednostek samorządu terytorialnego, dotyczące zagadnień związanych z rozwojem i standaryzacją budowy sieci SRP, bezpieczeństwem stacji końcowych, aktualizacją oprogramowania i doposażeniem urzędów. Utworzono forum internetowe w celu komunikacji i pomocy w ww. zakresie. W systemie ITSM *Atmosfera* została uruchomiona usługa umożliwiająca rejestrację przez użytkowników propozycji rozwojowych i udoskonaleń. W okresie marzec-sierpień 2015 r. COI przeprowadził cykl spotkań w pięciu USC w celu weryfikacji poprawności i efektywności działania BUSC oraz zebrania propozycji zmian w systemie.

W 2016 r. została zintensyfikowana współpraca robocza pomiędzy COI i MC oraz użytkownikami końcowymi w zakresie rozwoju SRP. Do 16 czerwca 2016 r. zostało przeprowadzone łącznie osiem spotkań grup roboczych z udziałem przedstawicieli COI.

23 marca 2016 r. została uruchomiona, obsługiwana przez COI, skrzynka e-mailowa *propozycje@coi.gov.pl,* służąca do zgłaszania propozycji usprawnień systemu.

Prace rozwojowe dotyczące SRP opierają się na katalogu zmian zweryfikowanych pod kątem formalno-prawnym i wykonalności technicznej przez MC i COI. Według informacji przekazanej przez Minister Cyfryzacji Panią Annę Streżyńską, na czerwiec 2016 r. katalog ten obejmował ponad 350 propozycji, z czego ok. 40% dotyczyło BUSC i był on na bieżąco aktualizowany. Odpowiedzi na zgłaszane przez użytkowników propozycje zmian były publikowane przez COI na stronie

internetowej[22] i przekazywane do dalszych prac. Poszczególnym zmianom nadawano priorytet pilności realizacji.

(dowód: akta kontroli str. 1709, 1712-1713, 2193-2194, 2197-2199, 2211-2311, 2342-2380, 2689-2725, 3844-3845, 3855-3859, 4329-4332, 4356, 4534, 4537)

1.8. Usługi elektroniczne świadczone z wykorzystaniem SRP

Opis stanu faktycznego

Na podstawie zlecenia nr 41/PLID/2015 udzielonego przez MSW w ramach umowy nr 4/DSiA/2013, COI zaprojektował i zrealizował oraz zgodnie z decyzją MSW, z dniem 1 marca 2015 r., udostępnił cztery e-usługi:

- *Sprawdź swoje dane w rejestrze PESEL,*
- *Sprawdź, czy dowód jest unieważniony,*
- *Sprawdź swoje dane w Rejestrze Dowodów Osobistych,*
- *Sprawdź, czy dowód osobisty jest gotowy.*

Ponadto, w 2015 r. zostały udostępnione przez MSW inne e-usługi umożliwiające:

- złożenie wniosku o wydanie dowodu osobistego,
- złożenie wniosku o wydanie odpisu aktu stanu cywilnego,
- zgłoszenie utraty lub uszkodzenia dowodu osobistego.

Usługi te nie wykorzystują jednak SRP bezpośrednio, powstały one poza zakresem programu *pl.ID.*

Wszystkie ww. e-usługi udostępnione zostały poprzez stronę internetową www.obywatel.gov.pl.

(dowód: akta kontroli str. 1583-1584, 1701-1819, 4321-4341, 4346-4362, 4704-4875)

Ocena cząstkowa

W ocenie NIK, COI wywiązał się z powierzonych mu zadań w zakresie budowy SRP, system został uruchomiony z dniem 1 marca 2015 r., jednak jego udostępnienie nastąpiło z opóźnieniem w stosunku do pierwotnej daty 1 stycznia 2015 r., zaś w SRP istniało wiele usterek rzutujących na sprawność pracy użytkowników końcowych w systemie.

Zdaniem NIK, przyczynami problemów z terminowym wdrożeniem systemu były zidentyfikowane przez użytkowników podczas testów liczne usterki w wytworzonym przez COI oprogramowaniu oraz niezrealizowanie przez COI części wymagań funkcjonalnych dla systemu. Opóźniło to odbiór przez MSW prac COI w zakresie kluczowych elementów systemu, tj. rejestrów PESEL, BUSC, RDO, Komponentu Niejawnego i aplikacji „Źródło".

Należy jednak wziąć pod uwagę, że rzetelną realizację zadań w zakresie budowy SRP utrudniały czynniki, na które COI nie miał bezpośredniego wpływu, m.in. narzucony krótki czas na zbudowanie systemu, rosnące w trakcie realizacji wymagania MSW i użytkowników końcowych oraz trwające równolegle do wytwarzania oprogramowania prace nad aktami prawnymi. Zdaniem NIK, do opóźnień w realizacji SRP przez COI przyczyniły się również przyjęte przez MSW rozwiązania z zakresu zarządzania programem *pl.ID* i niekonsekwentne ich stosowanie. Z kolei brak uwzględnienia przez MSW pilotażowego udostępnienia systemu, w ocenie NIK, uniemożliwił wykrycie i skorygowanie przed wdrożeniem SRP błędów i wad oprogramowania wytworzonego przez COI.

[22] https://www.coi.gov.pl/artykul/kolejne-propozycje-rozwoju-srp.html

Zdaniem NIK, przyjęta przez COI do wytwarzania SRP metodyka *Scrum* była adekwatna do uwarunkowań realizacji systemu, jednak korzyści z jej wykorzystania zostały ograniczone przez rezygnację przedstawicieli MSW z regularnego udziału w spotkaniach *Scrumowych*. Prowadziło to do sytuacji, w której weryfikacja funkcjonalności opracowanych przez COI następowała dopiero na etapie testowania, gdzie wprowadzanie zmian było utrudnione ze względu na ograniczenia czasowe i budżetowe.

W ocenie NIK, COI podjął działania zmierzające do zapewnienia rozwoju SRP, występując do MSW z propozycją przeznaczenia części zysku COI na działania rozwojowe oraz opracowując projekt ramowej umowy rozwojowej. W opinii NIK, działania polegające na aktywnym włączeniu użytkowników końcowych w prace rozwojowe oprogramowania SRP mogą pozytywnie wpłynąć na wyeliminowanie szeregu błędów zidentyfikowanych w działaniu systemu, a także ułatwić bieżącą modyfikację SRP w związku ze zmianami w przepisach prawa oraz wpłynąć na poprawę działania poszczególnych funkcjonalności wykorzystywanych przez użytkowników w trakcie obsługi spraw obywateli z wykorzystaniem SRP.

2. Wpływ wdrażania funkcjonalności i elementów SRP oraz zasilania tego systemu danymi na sprawność pracy użytkowników

2.1. Migracja danych do SRP

Opis stanu faktycznego

Zgodnie ze *Studium Wykonalności Projektu pl.ID* oraz zleceniami udzielonymi COI przez MSW w ramach umowy nr 4/DSiA/2013 na realizację SRP, masowa migracja danych została przewidziana m.in. dla modułów: PESEL i RDO. Masowa migracja danych nie obejmowała modułu BUSC i nie została przewidziana przez MSW w programie *pl.ID*. Jak wyjaśniła Wicedyrektor Pionu Projektów Kluczowych COI Pani Anna Jaczkowska, dane były migrowane do SRP z baz, z których migracja była możliwa (bazy sformalizowane), a w przypadku aktów stanu cywilnego, prowadzenie przez gminy rejestrów aktów stanu cywilnego w formie elektronicznej nie było obowiązkowe, aplikacje (tam gdzie były) nie były ujednolicone.

W ramach zlecenia nr 46 z dnia 28 lutego 2015 r., do umowy nr 4/DSiA/2013, MSW zleciło COI m.in. przeprowadzenie działań w zakresie migracji danych oraz udzielenie wsparcia technicznego i asysty merytorycznej w trakcie realizacji migracji. Wyniki przeprowadzonej migracji danych przedstawia poniższa tabela.

Rejestr (moduł SRP), do którego migrowano dane	Liczba rekordów zaimportowanych	Liczba rekordów niezaimportowanych	% rekordów niezaimportowanych
PESEL	502 061 359	454 840	0,1
RDO	160 574 941	770 032	0,5

Jak wynika z *Raportu końcowej migracji danych* z dnia 15 maja 2015 r., opracowanego przez COI, brak migracji wszystkich rekordów do poszczególnych rejestrów SRP wynikał m.in. ze słabej jakości danych źródłowych (rozbieżności i braku aktualnych danych) zgromadzonych w dotychczas wykorzystywanych bazach danych.

Jak ustalono w trakcie kontroli, w czerwcu 2016 r. COI zobowiązał się względem MC do przygotowania narzędzia do masowej migracji danych o aktach stanu cywilnego.

(dowód: akta kontroli str.13-214, 314-1279, 1576-1579, 1977-1983, 2379-2423, 2759-2762, 3800-3801, 3872-4316, 4672-4703, 4704-4875)

2.2. Zapewnienie sprawnego działania SRP

Opis stanu faktycznego

1. W dniu 30 czerwca 2016 r. pomiędzy MC a COI zawarta została umowa ramowa m.in. na świadczenie usług zapewniających poprawne i nieprzerwane funkcjonowanie SRP. Umowa została zawarta na okres od 1 lipca 2016 r. do 30 czerwca 2019 r. Wcześniej, w okresie od 1 marca 2015 r. do 30 czerwca 2016 r., COI utrzymywało SRP na podstawie czterech umów zawartych z MSW i MSWiA. W umowie z 30 czerwca 2016 r. zostały zdefiniowane minimalne wymagania Ministerstwa Cyfryzacji w odniesieniu do poziomu utrzymania SRP. I tak:

- dla procesu zarządzania incydentami określono maksymalny czas na rozwiązanie problemu wynoszący:
  - 3 dni robocze dla incydentu krytycznego (całkowita niedostępność funkcji jednego z modułów, dla którego nie ma obejścia i został zgłoszony przez co najmniej 5% lokalizacji),
  - 10 dni roboczych dla incydentu pilnego (niedostępność systemu i jego usług w co najmniej jednej lokalizacji),
  - 20 dni dla incydentu standardowego (nie powoduje niedostępności usług, ale oznacza ich nieprawidłowe działanie),
- dla procesu zarządzania problemem określono maksymalny czas jego obsługi wynoszący:
  - 40 dni roboczych dla problemu krytycznego,
  - 80 dni roboczych dla problemu pilnego,
  - 120 dni dla problemu standardowego,
- dla usługi serwisu oprogramowania określono gwarantowany czas naprawy błędów w nim stwierdzonych wynoszący:
  - 2 dni robocze dla błędu krytycznego,
  - 12 dni roboczych dla błędu pilnego,
  - 40 dni roboczych dla błędu standardowego.

Minimalna dostępność SRP została określona na poziomie 98%.

(dowód: akta kontroli str. 3489-3669, 4704-4875)

2. W dokumencie COI pn. *Procedury eksploatacyjne SRP* określony został sposób monitorowania działania SRP. W myśl tych zapisów monitorowaniu podlegają w szczególności:

- działanie serwisów systemów operacyjnych,
- dostęp do SRP pod kątem poszukiwania nieuprawnionych użytkowników lub prób włamań,
- stan działania aplikacji umożliwiających działanie SRP,
- bazy danych.

(dowód: akta kontroli str. 1573-1598, 4704-4875)

W COI monitoring działania SRP prowadzony jest przez Zespół Utrzymania Systemów, który przez 24 godziny na dobę monitoruje SRP i podejmuje działania, reagując na zdarzenia zachodzące w systemie.

(dowód: akta kontroli str. 1977-1983, 3489-3669, 3824-3834)

Ponadto, w COI istnieją procedury i instrukcje operacyjne, które zapewniają powtarzalne wykonywanie czynności w celu utrzymania gwarantowanego poziomu usług. Są nimi m.in. Procedura Zarządzania Poziomem Usług, która zawiera opisy ról i odpowiedzialności oraz opis procesu zarządzania poziomem usług, a także Instrukcja Zarządzania Poziomem Usług SRP opisująca m.in. cykliczne raportowanie poziomu usług dla SRP.

(dowód: akta kontroli str. 1966-1968, 1977-1983, 4704-4875)

3. Na zapewnienie przez COI dostępności SRP określonej przez MC na poziomie co najmniej 98% wpływ także mają usługi świadczone przez podmioty zewnętrzne. Umowy z dostawcami zewnętrznymi (łącznie 19 umów) w większości przypadków przewidują, że awarie mają być usuwane przez wykonawców w ciągu 24 godzin lub do końca następnego dnia roboczego od momentu zgłoszenia awarii; w przypadku dwóch umów awarie powinny być usunięte w ciągu 48 godzin. Zawarte przez COI umowy z dostawcami zewnętrznymi m.in. na dostawę sprzętu wraz ze wsparciem technicznym oraz na świadczenie usług telekomunikacyjnych zabezpieczają interesy COI, gdyż zapewniają możliwość monitorowania jakości dostarczanych usług wraz z możliwością naliczania kar umownych w przypadku niezachowania przez dostawców zamówionych parametrów tych usług.

(dowód: akta kontroli str. 1585-1588, 2957-3077, 3407-3488, 4704-4875)

4. W dniu 5 lutego 2014 r. Minister Spraw Wewnętrznych zawarł porozumienie z Komendantem Głównym Policji, którego przedmiotem było oddanie w użyczenie dla potrzeb SRP powierzchni w pomieszczeniu serwerowni oraz dwóch pomieszczeń biurowo-technicznych. W umowie określono m.in., że Minister Spraw Wewnętrznych ponosi koszty instalacji i napraw urządzeń serwerowni SRP oraz zapewnia ich sprawność i bezpieczeństwo. W umowie tej nie określono parametrów SLA dla pomieszczenia serwerowni (np. w odniesieniu do systemu nieprzerwanego zasilania, kontroli dostępu, klimatyzacji, zabezpieczeń przeciwpożarowych). Również w porozumieniu z dnia 29 czerwca 2016 r. zawartym pomiędzy MC a MSWiA, dotyczącym wykorzystania serwerowni na potrzeby SRP, nie wskazano parametrów SLA. Na podstawie zleceń udzielonych przez MSW w ramach umowy nr 4/DSiA/2013, COI dostarczył wyposażenie serwerowni. Z wyjaśnień Kierownika Zespołu Administratorów Systemów z COI, Pana Grzegorza Grabowskiego wynika, że serwerownie posiadają niezależne źródła zasilania zewnętrznego, zapasowe generatory, zasilacze awaryjne; dostarczanie zasilania i chłodzenia jest realizowane niezależnymi traktami. COI administruje systemami, których właścicielem jest MC, ale nie odpowiada w ramach zawartych umów za serwerownie, w tym za zapewnienie przestrzeni serwerowni, za zasilanie, za nadzór (bezpieczeństwo fizyczne), ani za żadne inne warunki (np. zapewnienie klimatyzacji). MC zapewnia serwerownie i jest właścicielem całej infrastruktury informatycznej, a COI nią administruje i zapewnia serwis dla sprzętu.

(dowód: akta kontroli str. 314-747, 1977-1983, 3824-3834, 4674-4875)

5. Na potrzeby SRP wykorzystywana jest sieć OST 112, której operatorem jest Policja nadzorowana przez MSWiA. Na podstawie umowy z 20 listopada 2014 r. zawartej pomiędzy Ministrem Spraw Wewnętrznych a EXATEL S.A.[23], za zapewnienie prawidłowego działania łączy dostępowych do OST 112 dla użytkowników SRP, odpowiada firma EXATEL S.A. Parametry dostępności sieci OST 112 zostały określone w załączniku nr 9 do ww. umowy. Dla ośmiu typów łącz tworzących sieć OST 112 określono maksymalny łączny czas niedostępność sieci, który wynosi od 360 do 1200 minut miesięcznie, co oznacza, że łącza te powinny

[23] Nr BAF-VI-2374-2-5/5-TK/2014 ze zm.

być dostępne odpowiednio od 97,22% do 99,17% w ciągu miesiąca. Ustalono, że faktyczny poziom dostępności sieci OST 112 w badanym okresie tj. od 1 marca 2015 r. do 31 lipca 2016 r. kształtował się na poziomie powyżej 98%, za wyjątkiem czterech miesięcy w 2015 r., w których poziom ten uległ obniżeniu. I tak, w maju wyniósł 92,36%, w czerwcu 97,75%, w lipcu 90,51%, natomiast we wrześniu 97,29%. Obniżona dostępność sieci OST 112 spowodowana była problemami z łączami.

(dowód: akta kontroli str. 1585-1588, 1977-1983, 3824-3834, 3872-4316, 4704-4875)

6. W załączniku nr 2 do umowy pomiędzy COI i MC na utrzymanie SRP nr 2/DIT/U/COI/2016 pn. *Katalog usług Systemu Informatycznego SRP* określono minimalną dostępność (na poziomie 98%) dla wszystkich usług realizowanych w ramach SRP oraz parametry czasowe świadczenia poszczególnych usług. COI w okresie od marca 2015 r. sporządzał dla Ministerstwa Spraw Wewnętrznych (od stycznia 2016 r. dla Ministerstwa Cyfryzacji) comiesięczne raporty dostępności poszczególnych usług SRP. Raporty za okres marzec – maj 2015 r. nie zawierały łącznych danych dotyczących dostępności całego SRP, natomiast dostępność dziewięciu z 205 usług tworzących SRP w okresie kwiecień-maj 2015 r. wyniosła poniżej 98%[24]. Ponadto, w raportach tych nie ujawniono zgłoszeń użytkowników dotyczących siedmiu problemów w funkcjonowaniu SRP, które miały wpływ na dostępność poszczególnych usług systemu (szczegółowy opis w punkcie dotyczącym uwag). Raporty za okres od czerwca 2015 r. do lipca 2016 r. wskazywały, że dostępność SRP kształtowała się na poziomie od 99,93% do 100%. NIK zauważa, że osiągnięta dostępność SRP nie oznacza, że działanie systemu było wolne od usterek/błędów, tylko że jego funkcje lub usługi były dostępne.

(dowód: akta kontroli str. 1585-1586, 3489-3669, 4704-4875)

Uwagi dotyczące badanej działalności

1. Biorąc pod uwagę społeczną istotność spraw związanych z rejestracją zdarzeń stanu cywilnego, NIK zwraca uwagę, że ustalone w umowie na utrzymanie SRP okresy rozwiązywania i usuwania incydentów (problemów) związanych z funkcjonowaniem SRP są zbyt długie. W takim stanie rzeczy zaistnienie krytycznego incydentu w funkcjonowaniu SRP może powodować w skali kraju trzydniową przerwę, uniemożliwiającą bieżącą rejestrację w SRP narodzin, małżeństw czy zgonów. W ocenie NIK, mając na uwadze, że COI jest jednostką państwową i odpowiada w ramach umowy na utrzymanie SRP za sprawność działania tego systemu, COI powinien zobowiązać się do rozwiązywania problemów w krótszych terminach, biorąc pod uwagę potrzeby użytkowników końcowych i obywateli.

(dowód: akta kontroli str. 3489-3669, 4704-4875)

2. NIK zwraca uwagę, że brak wskazania w umowach użyczenia powierzchni serwerowni na rzecz SRP parametrów technicznych SLA może utrudnić COI zapewnienie dostępności SRP na zamówionym przez MC poziomie 98%. Zdaniem NIK, aby mieć możliwość utrzymania dostępności SRP na określonym poziomie, COI powinien dążyć do uregulowania minimalnego poziomu dostępności serwerowni użyczonych przez MSWiA i Policję.

(dowód: akta kontroli str. 314-747, 1977-1983, 3824-3834, 4674-4875)

[24] W kwietniu 2015 r. dostępność usługi *Personalizacja dokumentów* wyniosła 95,3%; w maju 2015 r. dostępność następujących usług kształtowała się poniżej 98%: *Akceptacja wniosku o wydanie dowodu osobistego* 86,02%, *Personalizacja blankietów* 0%, *Wydawanie dowodów osobistych* 95,01%, *Obsługa migracji akt stanu cywilnego* 95,38%, *Obsługa działań administracyjnych w zakresie zarządzania kontami* 96,89%, *Rejestracja zameldowania na pobyt stały* 97,68%, *Przyjmowanie dowodu osobistego* 97,26%, *Łącze dedykowane* 92,36%.

3. NIK zwraca uwagę, że analiza incydentów zgłoszonych w okresie od 1 marca 2015 r. do 15 czerwca 2016 r. wykazała, iż miesięczne raporty z wykonania usług SRP sporządzane przez Kierownika Zespołu Zarządzania Usługami IT z COI, Panią Alicję Chylak nie odzwierciedlają dokładnej historii incydentów. Na przykład opisane w raporcie za miesiąc kwiecień 2015 r. obniżenie dostępności usługi *Personalizacja blankietów* dotyczyło zgłoszenia, które zostało zarejestrowane 6 marca 2015 r., problem został rozwiązany 18 kwietnia 2015 r., a zamknięcie zgłoszenia nastąpiło 28 kwietnia 2015 r. Wynika z tego, że obniżona dostępność usługi *Personalizacja blankietów* występowała w okresie od 6 marca do 18 kwietnia 2015 r., natomiast w raporcie za marzec 2015 r. dostępność tej usługi została określona na 100%. Nieścisłość wystąpiła także w przypadku obniżenia dostępności usługi *Obsługa działań administracyjnych* w raporcie za maj 2015 r. W tym przypadku zgłoszenie zostało zarejestrowane już 12 marca 2015 r. (rozwiązane i zamknięte 4 maja 2015 r.), a w raporcie za marzec 2015 r. dostępność tej usługi została określona na poziomie 100%. Stwierdzono jeszcze pięć innych przypadków raportowania bez uwzględnienia incydentów mających znaczenie dla poziomu dostępności SRP[25].

Ponadto, w raportach z usług utrzymania SRP wskazano, że problemy z dostępnością łącza występowały wyłącznie w maju, czerwcu i wrześniu 2015 r. podczas gdy z analizy rejestru incydentów wynika, że problemy z łączem wystąpiły również w marcu i grudniu 2015 r. (ponad 500 zgłoszeń) oraz w kwietniu 2015 r. (ponad 100 zgłoszeń).

Zdaniem NIK, COI w miesięcznych raportach z wykonania usług SRP powinno uwzględniać wszystkie czynniki wpływające na poziom dostępności usług SRP.

(dowód: akta kontroli str. 1585-1588, 4704-4875)

2.3. Organizacja wsparcia technicznego dla SRP

Opis stanu faktycznego

W strukturze organizacyjnej COI, w Pionie Eksploatacji Systemów funkcjonuje Zespół Service Desk, który realizuje wsparcie techniczne dla wszystkich systemów informatycznych utrzymywanych przez COI[26]. Wsparcie Zespołu Service Desk dla SRP jest realizowane od czerwca 2014 r. W Service Desk COI pracuje 25 osób posiadających wiedzę i doświadczenie umożliwiające obsługę zgłoszeń dotyczących SRP, z tego 14 osób bezpośrednio obsługuje zgłoszenia użytkowników SRP. Przed produkcyjnym uruchomieniem SRP, tj. przed 1 marca 2015 r., 12 pracowników świadczyło wsparcie dla przyszłych użytkowników SRP. Wsparcie obejmowało szkolenia, obsługę testów zewnętrznych i konfigurowanie stacji roboczych, przeglądarek i czytników, a także wsparcie dla Lokalnych Administratorów Ról w procesie nadawania uprawnień użytkownikom systemu.

(dowód: akta kontroli str. 1573-1598, 1832-1833, 2867-2874, 2925-2929, 3824-3834, 4704-4875)

---

[25] 1) Zgłoszenie 100612 (*Obsługa migracji aktów stanu cywilnego z postaci papierowej do systemu BUSC*), data zgłoszenia: 10 marca 2015 r., data rozwiązania: 30 kwietnia 2015 r., data zamknięcia zgłoszenia: 7 maja 2015 r. – obniżona dostępność usługi uwzględniona jedynie w raporcie za maj 2015 r.; 2) Zgłoszenie 93813 (*Wydawanie dowodu osobistego*), data zgłoszenia: 2 marca 2015 r., data rozwiązania: 19 maja 2015 r., data zamknięcia zgłoszenia: 19 maja 2015 r. – obniżona dostępność usługi uwzględniona jedynie w raporcie za maj 2015 r.; 3) Zgłoszenie 113502 (*Akceptacja wniosku o wydanie dowodu osobistego*), data zgłoszenia: 17 kwietnia 2015 r., data rozwiązania: 8 maja 2015 r., data zamknięcia zgłoszenia: 18 maja 2015 r. – obniżona dostępność usługi uwzględniona jedynie w raporcie za maj 2015 r.; 4) Zgłoszenie 103014 (*Personalizacja blankietów*), data zgłoszenia: 16 marca 2015 r., data rozwiązania: 11 maja 2015 r., data zamknięcia zgłoszenia: 11 maja 2015 r. – obniżona dostępność usługi uwzględniona jedynie w raportach za kwiecień i maj 2015 r.; 5) Zgłoszenie 93856 (*Przyjmowanie dowodu osobistego*), data zgłoszenia: 2 marca 2015 r., data rozwiązania: 11 maja 2015 r., data zamknięcia zgłoszenia: 11 maja 2015 r. – obniżona dostępność usługi uwzględniona jedynie w raporcie za maj 2015 r.

[26] M.in. SRP, Centralnej Ewidencji Pojazdów i Kierowców, elektronicznej Platformy Usług Administracji Publicznej, systemu do zarządzania dokumentami - eDOC, Centralnej Ewidencji Wydanych i Unieważnionych Dokumentów Paszportowych, Publikatora Aktów Prawnych i innych mniejszych systemów.

Do zgłaszania problemów w działaniu SRP, COI udostępnił użytkownikom końcowym SRP System ITSM[27] pod nazwą *Atmosfera*. System ten umożliwia zarządzanie zgłoszonymi przez użytkowników problemami (incydentami) 24 godziny przez 7 dni w tygodniu[28] poprzez stronę internetową[29]. Dodatkowo dla dokonywania zgłoszeń udostępniona została linia telefoniczna oraz adres mailowy - obsługiwane również przez zespół konsultantów COI. Wpływające zgłoszenia o problemach (incydentach) są obsługiwane przez pracowników Zespołu Service Desk od poniedziałku do piątku w godz. 7-19 (administratorzy SRP są dostępni od poniedziałku do piątku w godz. 8-16). W przypadku zgłoszenia, które wpłynie poza standardowymi godzinami pracy Zespołu Service Desk jest ono obsługiwane od następnego dnia roboczego. W przypadku awarii krytycznej (gdy system jest niedostępny) administratorzy pracują nad rozwiązaniem problemu całą dobę, również w dni wolne od pracy.

(dowód: akta kontroli str. 2867-2874, 3824-3834, 4704-4875)

Jak wyjaśnił Zastępca Dyrektora COI Pan Andrzej Pieczunko, po zarejestrowaniu zgłoszenia, użytkownik ma możliwość przesłania za pośrednictwem ITSM *Atmosfera* dwóch rodzajów komunikatów dotyczących zgłoszenia: ponaglenia (w celu przyspieszenia obsługi) lub sprostowania (w celu przekazania dodatkowych informacji dotyczących przedmiotu zgłoszenia). Wraz z zamknięciem obsługi incydentu użytkownik otrzymuje e-mail z prośbą o potwierdzenie rozwiązania wraz z linkiem odsyłającym do zgłoszenia gdzie ma możliwość potwierdzenia poprawności jego realizacji. Według wyjaśnień, p.o. Kierownika Zespołu Service Desk z COI, Pani Anny Olek w przypadku braku kontaktu z użytkownikiem, zgłoszenie zostaje zamknięte automatycznie po siedmiu dniach roboczych od daty rozwiązania zgłoszenia.

(dowód: akta kontroli str. 1573-1598, 1861-1866, 2763-2769, 2867-2874, 3824-3834, 4704-4875)

Obowiązująca w COI *Procedura Zarządzania Incydentem* wyodrębnia trzy linie wsparcia. I tak:

- pracownicy pierwszej linii wsparcia należą do Zespołu Service Desk i odpowiadają za rejestrowanie, kategoryzację i priorytetyzację incydentów, świadczenie wsparcia w ramach I linii dla użytkowników, analizowanie i rozwiązywanie lub eskalowanie incydentów, monitorowanie całego cyklu obsługi incydentu, a także dokumentowanie informacji, aktywności oraz rozwiązań. W ramach pierwszej linii wsparcia w COI zgłoszenia obsługuje 10 osób;
- drugą linię wsparcia tworzy zespół analityczno-merytoryczny Service Desk oraz pozostałe zespoły IT w COI. Wydzielone są tzw. zespoły wsparcia, które składają się z pracowników COI (czasem z różnych komórek organizacyjnych). Zgodnie z załącznikiem nr 1 do *instrukcji obsługi incydentu pl.ID* specjalista drugiej linii wsparcia odpowiada za analizowanie, rozwiązywanie incydentów przekazanych przez pierwszą linię wsparcia, jeżeli nie posiada odpowiednich kompetencji do obsługi zgłoszenia przekazuje je do trzeciej linii wsparcia (tzw. eskalowanie obsługi incydentów);
- trzecią linię wsparcia w ramach infrastruktury SRP stanowią zewnętrzni dostawcy elementów infrastruktury lub oprogramowania (IBM, Hitachi, Oracle, Linux Polska), którzy na podstawie umów gwarancyjnych lub pogwarancyjnych

[27] Ang. IT Services Management – zarządzanie usługami IT.
[28] Za wyjątkiem krótkich przerw serwisowych.
[29] https://pomoc.coi.gov.pl

zawartych z COI, świadczą usługi wsparcia w zakresie sprzętu i oprogramowania. W zakresie aplikacji trzecią linię wsparcia realizuje Pion Rozwoju Systemów COI.

Wszelkie problemy związane z działaniem sieci OST 112 są zgłaszane przez COI do MSWiA. Kierownik Zespołu Administratorów Systemów z COI, Pan Grzegorz Grabowski wyjaśnił, iż COI monitoruje dostępność łączy końcowych, odbiera zgłoszenia od użytkowników i przekazuje je do MSWiA, które odpowiada za utrzymanie sieci OST 112.

(dowód: akta kontroli str. 1573-1598, 1977-1983, 2867-2874, 2925-2929, 3824-3834, 3872-4316, 4704-4875)

2.4. Obsługa zgłoszeń użytkowników o problemach w funkcjonowaniu SRP, zarejestrowanych w systemie ITSM *Atmosfera*

Opis stanu faktycznego

Badaniem objęto 40 197 incydentów zgłoszonych przez użytkowników SRP w okresie od 1 marca 2015 r. do 15 czerwca 2016 r. Badanie wykazało, że 38 721 zostało rozwiązanych (96,3%). Natomiast w przypadku 369 zgłoszeń ich realizacja została czasowo wstrzymana i oczekuje na wznowienie, a 1 106 incydentów posiadało status „Otwarte", tj. są aktualnie rozwiązywane.

Analiza zgłoszonych problemów (incydentów) zarejestrowanych przez Service Desk COI w ww. okresie wykazała, że 23,6% incydentów rozwiązano w ciągu godziny od jego zgłoszenia; 14,1% - w ciągu doby; 14,7% - do tygodnia; 23,3% - do miesiąca, a 15% - do trzech miesięcy. Należy przy tym wskazać, że na rozwiązanie 9,3% incydentów Service Desk COI potrzebował do roku czasu.

Według stanu na dzień 15 czerwca 2016 r., na rozwiązanie oczekiwało 1 106 zgłoszeń problemów o statusie „Otwarte", z tego 0,5% zgłoszono do 24 godzin, 3,2% do tygodnia, 8,7% do miesiąca, 22,1% do trzech miesięcy, 59,9% do roku czasu, a 5,7% zgłoszeń wpłynęło do COI ponad rok temu. Analiza ww. 1 106 zgłoszeń pozostających jako otwarte wykazała, że 703 zgłoszenia miały charakter incydentalny (63,6%), a pozostałe 403 były powtarzalne.

Jak wskazała w wyjaśnieniach Specjalista Service Desk z COI, Pani Anna Saramonowicz, utrudnieniem w sprawnym rozwiązywaniu części zgłoszonych problemów jest komunikacja z Ministerstwem (dawniej MSW, obecnie MC), gdyż czas odpowiedzi na pytania skierowane do Ministerstwa wyjątkowo jest krótszy niż dwa miesiące, a ponadto odpowiedzi są ogólnikowe.

(dowód: akta kontroli str. 1573-1578, 4704-4875)

Uwagi dotyczące badanej działalności

W ocenie NIK, zapewnione przez COI wsparcie techniczne SRP umożliwiało rozwiązywanie problemów, ale terminy ich rozwiązywania, zwłaszcza w pierwszych miesiącach po uruchomieniu systemu były zbyt długie. Przez pierwsze 9 miesięcy rozwiązanie ponad 43% zgłoszeń zajmowało przynajmniej 1 miesiąc (w pierwszym miesiącu działania dotyczyło to aż 56% zgłoszeń). Oznacza to, że zgłoszenia nie były obsługiwane na bieżąco, a użytkownicy doświadczali utrudnień w realizacji ich bieżących zadań. Efektywność wparcia technicznego SRP ulegała stopniowej poprawie, lecz dopiero w czerwcu 2016 r. wsparcie techniczne, zdaniem NIK, zaczęło funkcjonować skutecznie. Świadczy o tym fakt, że 83,6% incydentów rozwiązywano w ciągu jednego dnia, w tym 60,8% z nich rozwiązywano już w ciągu godziny. Przyczyną dużej liczby zgłoszeń w początkowym okresie eksploatacji było przedwczesne uruchomienie SRP. System nie był wówczas wystarczająco

przetestowany, ani nie posiadał wszystkich wymaganych funkcjonalności, w szczególności w zakresie modułu BUSC i aplikacji „Źródło". W efekcie pierwsza linia wsparcia nie znając rozwiązania problemu nie mogła skutecznie udzielić pomocy użytkownikom (czyli nie spełniała funkcji zapory przed nadmierną liczbą zgłoszeń kierowanych do kolejnych linii), gdyż niezbędne było do tego działanie drugiej, a niekiedy też trzeciej linii wparcia. Te zaś uległy przeciążeniu wskutek realizacji zbyt dużej liczby zgłoszeń. Jednocześnie wiele zgłoszeń nie mogło zostać rozwiązanych, gdyż wymagały podjęcia decyzji o dokonaniu istotnych zmian w systemie, a zaznaczyć należy, że pierwsza linia wsparcia nie dysponuje możliwością skorygowania działania systemu, czy usunięcia usterki – może jedynie poinstruować użytkowników odnośnie właściwego sposobu postępowania w danych okolicznościach. Istotny w tym zakresie był też brak przez pierwszy rok eksploatacji umowy rozwojowej SRP, która pozwoliłaby na rozwiązanie wielu problemów. Na sprawność wsparcia technicznego wpływ miał także długi czas korespondencji z właścicielem systemu (najpierw MSW, a potem MC).

(dowód: akta kontroli str. 1573-1578, 4704-4875)

2.5. Baza wiedzy dla użytkowników SRP

Opis stanu faktycznego

COI opracował i udostępnił poprzez stronę internetową *http://plid.obywatel.gov.pl/pliki-urzednik* tzw. Centrum Pomocy dla użytkowników SRP. Zastępca Dyrektora COI Pan Andrzej Pieczunko wyjaśnił, że *kompletne informacje o stronie, jej zawartości, treściach na niej publikowanych były propagowane wśród użytkowników końcowych podczas konferencji, szkoleń, spotkań w gminach, za pośrednictwem Newslettera, forum oraz mediów. Ponadto, informacja ta była wielokrotnie przekazywana Lokalnym Administratorom Systemu, chociażby poprzez fakt, że na stronie były publikowane różnorodne ankiety.* (…) *Aktualnie COI nie prowadzi działań informacyjnych o możliwości korzystania z informacji w ramach Centrum Pomocy funkcjonującego na stronie plid.obywatel.gov.pl, ani nie prowadzi aktualizacji tej zakładki. W Zleceniu nr 38/PLID/2013 termin zakończenia tych działań przez COI został określony na 25 marca 2015 r. COI pismem znak COI-ZPLID.0500.14.39.2013.TP/45 z 25 marca 2015 r. poinformował Ministerstwo Spraw Wewnętrznych o zakończeniu bieżącej obsługi strony. Od tego momentu za merytoryczną aktualizację strony i inne działania z nią związane odpowiadało MSW a obecnie Ministerstwo Cyfryzacji. Obok Newslettera do LAS-ów, informującego o nowych wdrożeniach, minimum jeden raz w miesiącu wysyłany jest Newsletter informacyjny do bazy kilkunastu tysięcy urzędników.* Ponadto, zgodnie z wyjaśnieniami udzielonymi przez Zastępcę Kierownika Zespołu Service Desk z COI, Pana Piotra Ślawskiego, *w zespole Pionu Rozwoju Systemu (PRS) jest zespół analityków, który tworzy instrukcje, jak posługiwać się nowymi funkcjami aplikacji. Instrukcje są opiniowane przez Ministerstwo. Po zaakceptowaniu są zapisywane w plikach PDF i są udostępniane LAS'om w bazie wiedzy. (…) Instrukcja dotycząca zmian jest rozsyłana w formie newslettera. Lista instrukcji liczy 19 artykułów*.

(dowód: akta kontroli str. 314-747, 755-1279, 2763-2769, 2867-2874, 4704-4875)

2.6. Procedury awaryjne SRP

Opis stanu faktycznego

Zasady postępowania w przypadku sytuacji awaryjnych zostały opisane przez COI w dokumencie *Procedury awaryjne SRP*. Dokument ten opisuje procedurę postępowania w przypadku awarii ośrodka przetwarzania danych, pojedynczego

serwera aplikacyjnego, serwera DNS, baz danych, fizycznego serwera Blade oraz sprzętowej awarii serwera Power.

Kierownik Zespołu Administratorów Systemów z COI, Pan Grzegorz Grabowski poinformował, że przełączenia serwerów podstawowych były dokonywane w trakcie prac administracyjnych i zakończyły się sukcesem.

(dowód: akta kontroli str. 1966-1968, 1977-1983, 4672-4682, 4704-4875)

W COI utrzymaniem SRP zajmuje się Zespół Utrzymania Systemów, który pracuje w systemie zmianowym 12-godzinnym, i jak wyjaśnił Kierownik Zespołu Utrzymania Systemów z COI, Pan Michał Kosmowski, na każdej zmianie są cztery osoby. W przypadku awarii krytycznych poza standardowymi godzinami pracy Zespół Utrzymania Systemów kontaktuje się z administratorami, którzy podejmują stosowne działania.

Z analizy kart osobowych wynika, że utrzymaniem systemów, w tym SRP, zajmowało się łącznie 59 pracowników COI.

(dowód: akta kontroli str. 1576-1579, 1825-1833, 3824-3834, 4704-4875)

W dokumencie opracowanym przez COI pn. *Procedury eksploatacyjne SRP* zawarto zasady postępowania przy najczęściej występujących (typowych) awariach SRP, a w systemie ITSM *Atmosfera* dostępne są instrukcje zawierające opis działań, które powinny być podjęte w celu usunięcia takich awarii, co sprzyja szybszemu usuwaniu typowych awarii.

(dowód: akta kontroli str.1964-1965, 2867-2874, 3824-3834, 4704-4875)

2.7. Zarządzanie przestrzenią dyskową SRP

Procedury obowiązujące COI przewidywały monitorowanie pojemności nośników pamięci SRP oraz informowanie Zespołu Utrzymania Systemów COI o konieczności podjęcia działań w związku z wyczerpywaniem się przestrzeni dyskowej przeznaczonej dla SRP. Zasady monitorowania pojemności nośników pamięci zostały opisane w dokumencie *Procedury eksploatacyjne SRP*. W pkt 1.6 tych procedur pn. *Kontrolowanie procentowej zajętości systemów plików* określono, że monitorowanie zajętości przestrzeni dyskowej jest realizowane z wykorzystaniem narzędzia *ManageEngine*, gdzie wprowadzone są następujące progi ostrzegawcze: warning – 75% i critical – 85% zajętości określonej przestrzeni dyskowej.

(dowód: akta kontroli str. 1966-1968, 3824-3834, 4704-4875)

2.8. Zapewnienie prawidłowości danych zgromadzonych w rejestrach SRP

Opis stanu faktycznego

W SRP funkcjonują zapewnione przez COI mechanizmy sprawdzania prawidłowości danych wprowadzanych do tego systemu (tzw. walidacja danych). Zasady walidacji zostały opisane w *Dokumentacji powykonawczej SRP*, zgodnie z którą dane wprowadzane do SRP są w pierwszej kolejności weryfikowane na podstawie reguł walidacji. Dalszym poziomem weryfikacji danych są mechanizmy systemów zarządzania bazami danych, tzw. mechanizm kluczy obcych, określenie typów pól i mechanizm ograniczeń.

W kwestii zapewnienia spójności i poprawności danych w SRP, Kierownik Zespołu Produkcji Oprogramowania II z COI, Pan Teodor Buchner wyjaśnił, że *w toku prac nad migracją danych ujawniło się wiele błędów w danych. (…) Rezygnacja z walidacji konkretnych danych była uzgadniania z klientem (MSW). Pewne*

mechanizmy są cały czas aktywne. Wskazał też, że *COI wnioskuje od dłuższego czasu o zlecenie w celu kompleksowej naprawy błędów w danych. O części błędów było informowane Ministerstwo Spraw Wewnętrznych i Ministerstwo Cyfryzacji. Istnieją w danych błędy biznesowe wynikające np. z braku standaryzacji kodów pocztowych. W danych historycznych można było mieć adres, który nie istnieje*.

Kierownik Zespołu Architektury i Standardów IT z COI, Pan Piotr Dudzic wyjaśnił, że *były sytuacje, w których mechanizmy walidacji musiały zostać zdjęte z powodu niespójności danych historycznych. Takie decyzje były każdorazowo uzgadniane z MSW. W niektórych przypadkach nadawanie numerów PESEL odbywało się bez dostępu do systemu (Jantar). Numery sekwencyjne były wtedy celowo zawyżane (…), aby uniknąć konfliktów. Dokonano sprawdzenia i ustalono, że w systemie nie ma dwóch różnych osób o tym samym numerze PESEL (ograniczenie twarde w bazie danych) oraz niezgodności cyfry kontrolnej. Błędy typowe to – braki danych (np. nazwiska rodowego), literówki, błędy w danych słownikowych, błędy w numerach PESEL (część oparta na dacie nie pasuje do daty z kalendarza). Zdarza się, że bazy nie miały zachowanych więzów referencyjnych (np. dowód osobisty i osoba – dowody są przypisane do niewłaściwych osób). (…) Niektóre błędy uniemożliwiły migrację niektórych danych.*

Wprowadzenie SRP ujawniło szereg rozbieżności w danych zmigrowanych do SRP. COI wprowadziło w SRP mechanizmy weryfikacji danych znajdujących się w poszczególnych rejestrach wchodzących w skład SRP.

(dowód: akta kontroli str. 1964-1965, 1977-1983, 4688-4875)

Z *Dokumentacji powykonawczej SRP* opracowanej przez COI wynika, że SRP wykorzystuje przede wszystkim wewnętrzne źródła danych słownikowych[30]. Jedynym słownikiem zewnętrznym, z którego korzysta SRP jest słownik podziału terytorialnego kraju „TERYT" udostępniany przez Główny Urząd Statystyczny. Na podstawie analizy dokumentacji powykonawczej SRP ustalono, że COI opracował aplikację służącą do korzystania z zewnętrznych źródeł danych słownikowych. Aplikacja umożliwia import słowników w określonych formatach z dostępnych źródeł.

(dowód: akta kontroli str. 1573-1598, 1964-1965, 1977-1983, 3800-3801, 3824-3834, 4704-4875)

2.9. Zarządzanie zmianami w systemie informatycznym SRP

Opis stanu faktycznego

Sposób dokonywania zmian w systemie informatycznym SRP został opisany w dokumencie przygotowanym przez COI pn. *Instrukcja Zarządzania Zmianą SRP*. Zgodnie z *Instrukcją*, w przypadku potrzeby wprowadzania zmian, postępowanie rozpoczyna się od sporządzenia wniosku o zmianę. Proces przeprowadzenia zmiany rozpoczyna się od jej rejestracji, poprzez jej zaopiniowanie i zaakceptowanie przez menedżera zmian w SRP oraz Radę ds. Zmian[31] i kończy się na wdrożeniu zmiany wraz z jej przeglądem i ostatecznym zamknięciem. Każda zmiana nie będąca zmianą standardową musi uzyskać akceptację MC. Na podstawie zarejestrowanego wniosku o zmianę, menedżer zmian w SRP przygotowuje harmonogram/plan wprowadzenia zmiany. Plan ten jest synchronizowany z planem dostępności usług, w celu jak największego zminimalizowania konfliktów mogących wyniknąć pomiędzy wprowadzanymi zmianami, a udostępnianymi już usługami IT[32].

[30] Zamknięty katalog danych możliwych do wykorzystania w ramach operacji wykonywanych z wykorzystaniem aplikacji „Źródło".

[31] Rada ds. Zmian jest zespołem doradczym i opiniującym każdą zmianę z wyłączeniem zmian standardowych.

[32] Tzn. systemami informatycznymi stanowiącymi funkcjonalnie całość.

Opracowywanie i testowanie zmian dokonywane jest w COI z wykorzystaniem oddzielnych środowisk, wprowadzanie zmian do środowiska produkcyjnego realizowane jest w ramach kolejnych wydań/nowych wersji SRP.

Analiza zmian w SRP dokonanych w okresie od lutego 2015 r. do sierpnia 2016 r. wykazała, że większość wprowadzanych modyfikacji miała na celu usunięcie usterek, które ujawniły się po uruchomieniu SRP. Usterki te dotyczyły różnego typu błędów w funkcjonalnościach SPR, jak np. błędnego zapisu danych, błędów w raportach, czy błędnego zachowania aplikacji „Źródło". W innych przypadkach modyfikacje zmierzały do poprawy wydajności systemu, jak np. w zakresie funkcji unieważniania dowodu. Inne modyfikacje dotyczyły wprowadzenia nowych funkcjonalności lub rozszerzenia funkcjonalności już istniejących[33] i miały miejsce pod koniec wskazanego powyżej okresu. Powyższe wskazuje, że jakość systemu w chwili uruchomienia nie była zadowalająca.

(dowód: akta kontroli str. 1587-1588, 1966-1968, 2888-2889, 4704-4875)

Wyniki kontroli wykazały, że środowiska testowe SRP służące do badania, weryfikowania projektowanych zmian są adekwatne pod względem konfiguracji ich oprogramowania do środowiska rzeczywistego.

(dowód: akta kontroli str. 1977-1983, 3824-3834, 4704-4875)

2.10. Szkolenia użytkowników SRP

Opis stanu faktycznego

W związku z przygotowaniem i udostępnieniem SRP COI realizował bezpłatne szkolenia dla użytkowników końcowych programu *pl.ID*. Szkolenia były prowadzone według modelu hybrydowego, polegającego na połączeniu jednodniowych, stacjonarnych warsztatów bezpośrednich dla liderów z gmin i urzędów stanu cywilnego (po jednej osobie z każdej jednostki) z indywidualnymi szkoleniami online dla wszystkich użytkowników[34].

W okresie od 1 lipca 2014 r. do 27 listopada 2014 r. COI prowadził szkolenia stacjonarne dla tzw. liderów. Składały się z części teoretycznej (obejmującej m.in. cele programu *pl.ID*, zasady funkcjonowania SRP, najważniejsze zmiany prawne oraz zasady bezpieczeństwa przetwarzania danych) oraz z ćwiczeń praktycznych polegających na wykonywaniu wybranych czynności związanych z praktycznym wykorzystaniem SRP. W szkoleniach dla liderów wzięło udział 4 167 urzędników. Szkolenia z zakresu PESEL i RDO zostały ocenione dobrze przez 90% uczestników, natomiast szkolenia z BUSC dobrze oceniło 64% szkolonych, a 21% osób podało odpowiedź „trudno powiedzieć". Większość uczestników szkoleń pozytywnie oceniła aplikację „Źródło"[35].

W okresie od 13 sierpnia 2014 r. do 25 marca 2015 r. COI udostępnił użytkownikom końcowym możliwość szkolenia w formie e-learningu[36]. Użytkownicy mieli dostęp m.in. do filmów instruktażowych, podręczników szkoleniowych, zestawów ćwiczeń i testów samosprawdzających. Z tej formy szkolenia skorzystało 11 625 użytkowników[37]. Szkolenia z zakresu działania: modułu RDO pozytywnie oceniło 78% szkolonych, modułu PESEL – 82% uczestników szkoleń, natomiast z zakresu

---

33 Np. narzędzie skryptowe umożliwiające zwracanie danych dla wielu rekordów osób na podstawie pliku wejściowego, co usprawniło i zautomatyzowało proces pozyskiwania danych.

34 Dla przedstawicieli MSW, Centrum Personalizacji Dokumentów, Agencji Bezpieczeństwa Wewnętrznego, Poltransplantu (użytkownika Centralnego Rejestru Sprzeciwów), Kancelarii Prezydenta RP (użytkownika Systemu Odznaczeń Państwowych) COI przeprowadził szkolenia dedykowane. Łącznie w szkoleniach dedykowanych uczestniczyło 170 osób.

35 Obszar: „podpowiedzi aplikacji" pozytywnie oceniło 70% respondentów, „wygląd" – 70% respondentów, „szybkość znajdowania funkcjonalności" – 66% respondentów, „łatwość orientacji oraz obsługi" – 67%.

36 https://szkolenia.obywatel.gov.pl

37 Według *Raportu końcowego z realizacji zlecenia nr 24/PLID/2013* z 21 kwietnia 2015 r.

działania modułu BUSC – pozytywnie oceniło tylko 58% biorących udział w szkoleniu. 19% osób uczestniczących w szkoleniu z modułu BUSC stwierdziło, że zasady działania tego modułu są niezrozumiałe, a kolejne 23% szkolonych nie miało zdania na ten temat.

Użytkownikom SRP została udostępniona także szkoleniowa wersja aplikacji „Źródło”[38], w której na dzień 30 grudnia 2014 r. zarejestrowało się 8187 użytkowników[39].

Dyrektor COI Pan Rafał Leśkiewicz poinformował, że zakres każdego szkolenia był proponowany MSW przez COI i zatwierdzany w trybie roboczych ustaleń.

W dniach 10-12 grudnia 2014 r. oraz 19-23 stycznia 2015 r. COI zorganizował dla użytkowników SRP egzamin ze znajomości obsługi systemu. Polegał on na wykonaniu w aplikacji szkoleniowej „Źródło” zadań praktycznych z zakresu modułów PESEL, RDO lub BUSC (do wyboru w zależności od obszaru w jakim urzędnik wykonuje swoje obowiązki służbowe). Egzamin zaliczyło 10 025 użytkowników SRP, przy czym jedna osoba mogła zdawać od jednego do trzech egzaminów, tj. dla każdego modułu odrębnie. Łączna liczba wszystkich zdanych egzaminów wyniosła 19 327[40].

Za realizację całego procesu szkoleń w ramach zlecenia nr 24/PLID/2013 COI otrzymał wynagrodzenie w wysokości 3 510,9 tys. zł brutto.

Po wdrożeniu SRP COI zorganizował odpłatne szkolenia dla użytkowników końcowych SRP z jednostek samorządu terytorialnego. Dyrektor COI Pan Rafał Leśkiewicz poinformował, że decyzja o prowadzeniu takich szkoleń wynikała z faktu, że *po uruchomieniu SRP 1 marca 2015 r. COI otrzymywał wiele sygnałów z gmin, że istnieje potrzeba dodatkowych szkoleń obsługi aplikacji, a jednocześnie ustalono, że w zakresie możliwości finansowych projektu ani budżetu MSW nie leżała wówczas możliwość zlecenia tych prac COI przez MSW. Dodatkowo COI uzyskał informacje, że takie szkolenia zaczynają być oferowane przez podmioty zewnętrzne*. *Zakres odpłatnych szkoleń został określony na podstawie pytań zgłaszanych przez urzędników do Service Desk oraz drogą telefoniczną. W czerwcu 2015 r. trwały prace COI nad opracowaniem programu i konsultacje z gminami i urzędami wojewódzkimi w zakresie potrzeb.*

Odpłatność za przeszkolenie jednego użytkownika SRP wynosiła 400 zł. W trakcie 53 szkoleń zostało przeszkolonych 802 pracowników jednostek samorządu terytorialnego. Szkolenia były prowadzone przez pracowników COI w ramach ich obowiązków służbowych.

Na podstawie umowy na utrzymanie SRP nr 2/DIT/U/COI/2016 zawartej w dniu 30 czerwca 2016 r. pomiędzy MC a COI, COI zostało powierzone zadanie realizacji szkoleń, w tym m.in. przygotowywanie scenariuszy filmów szkoleniowych dla użytkowników aplikacji „Źródło”, nagrywanie filmów szkoleniowych i zamieszczanie ich na kanale YouTube, prowadzenie szkoleń dla urzędników korzystających z aplikacji „Źródło” w miejscu ich pracy oraz prowadzenie warsztatów szkoleniowych dla urzędników zgodnie z zapotrzebowaniem zgłaszanym przez poszczególne jednostki.

(dowód: akta kontroli str. 1569-1575, 1591-1700, 1843-1860, 1943-1944, 3489-3669)

---

38 https://szkolenia-zrodlo.obywatel.gov.pl

39 Według *Raportu końcowego z realizacji zlecenia nr 24/PLID/2013* z 21 kwietnia 2015 r.

40 Egzamin z modułu PESEL zdało 7 100 użytkowników, z modułu RDO – 6 745 użytkowników, z modułu BUSC – 5 482 użytkowników.

Ocena cząstkowa

W ocenie NIK, wsparcie techniczne dla użytkowników SRP zostało zorganizowane zgodnie ze współczesną praktyką w tym zakresie. Zdaniem NIK, czas oczekiwania na rozwiązanie części zgłoszeń o problemach w działaniu SRP był zbyt długi i w skrajnych przypadkach sięgał ponad roku, rozwiązanie niektórych problemów uzależnione było od wielu czynników, m.in. od uzyskania od MSW i MC interpretacji określonych przepisów prawnych. W opinii NIK, określony przez MC w umowie na utrzymanie SRP czas na usunięcie przez COI awarii tego systemu jest zbyt długi z punktu widzenia potrzeb użytkowników SRP, a także potrzeb obywateli (trzy dni robocze w przypadku incydentu krytycznego).

Kontrola wykazała, że określony przez właściciela SRP (MC, wcześniej MSW) poziom dostępności systemu (98%) został osiągnięty w okresie objętym kontrolą. Należy przy tym zauważyć, że w niektórych raportach COI o dostępności usług SRP wskazywano, że usługi były dostępne na poziomie 100%, podczas gdy informacje zgromadzone w oprogramowaniu ITSM *Atmosfera* wskazywały, że występowały istotne problemy w dostępności niektórych usług.

COI zobowiązując się do zapewnienia dostępności SRP na poziomie 98% powinien dążyć do określenia wymaganych parametrów SLA dla wszystkich usług i elementów infrastruktury mających wpływ na dostępność SRP, w tym także serwerowni, gdyż brak regulacji może utrudnić COI zachowanie wymaganej dostępności SRP.

W ocenie NIK, opracowane i stosowane przez COI procedury eksploatacyjne i awaryjne pozwalają na zapewnienie ciągłości działania SRP. W opinii NIK, zmiany w oprogramowaniu były odpowiednio testowane, na środowisku testowym o odpowiednich parametrach. Stosowane przez COI mechanizmy wdrażania zmian w oprogramowaniu SRP były właściwe, bowiem pozwalały na zminimalizowanie negatywnego wpływu tych zmian na usługi już funkcjonujące w środowisku produkcyjnym. W COI zorganizowano proces zarządzania zmianami w SRP. Wprowadzanie zmian w systemie odbywa się w ramach zdefiniowanego, kontrolowanego procesu, w którym zmiany są zatwierdzane przez właściciela systemu, a ich wykonawcą jest COI.

W opinii NIK, szkolenia zorganizowane przez COI umożliwiły użytkownikom SRP właściwe przygotowanie się do pracy w udostępnionym systemie, a tworzone i zamieszczane w bazie wiedzy przez COI instrukcje ułatwiają użytkownikom posługiwanie się nowymi funkcjami w SRP.

3. Zapewnienie bezpieczeństwa SRP i jego danych

3.1. Zarządzanie bezpieczeństwem SRP

Opis stanu faktycznego

COI stanowi pierwszą linię w zarządzaniu bezpieczeństwem SRP, realizując podstawowe procedury reagowania na incydenty bezpieczeństwa, natomiast bardziej zaawansowane działania będące reakcją na te incydenty realizuje MC we współpracy z CERT[41] i Agencją Bezpieczeństwa Wewnętrznego.

Zadania COI w zakresie zarządzania bezpieczeństwem SRP określone zostały w umowach z MSW/MSWiA/MC na utrzymanie SRP. Zakres zadań powierzonych COI obejmował m.in. monitorowanie bezpieczeństwa systemu, zapewnienie bezpieczeństwa zmian oraz zarządzanie incydentami bezpieczeństwa.

[41] Rządowy Zespół Reagowania na Incydenty Komputerowe.

Zarządzanie bezpieczeństwem systemu SRP realizowane było w oparciu o *Politykę Bezpieczeństwa rejestrów państwowych w MSW objętych projektem pl.ID*[42], opracowaną przez Departament Teleinformatyki MSW (dalej: *Polityka Bezpieczeństwa pl.ID*). Celem wprowadzonej *Polityki Bezpieczeństwa pl.ID* było zapewnienie integralności, poufności, rozliczalności, niezaprzeczalności i niezawodności zasobów wchodzących w skład środowiska pl.ID oraz zagwarantowanie stałej dostępności świadczonych usług, a w szczególności zapewnienie wymaganego poziomu bezpieczeństwa i niezawodności przetwarzania informacji niezbędnych do sprawnej realizacji zadań z zakresu rejestrów państwowych.

(dowód: akta kontroli str. 1284-1427, 3338-3351, 3824-3834, 4321-4345, 4376-4516, 4527-4547, 4665-4671, 4683-4875)

Uwagi dotyczące badanej działalności

Zdaniem NIK, COI przyjęło do realizacji zadania w zakresie zarządzania bezpieczeństwem SRP w sytuacji gdy system zarządzania bezpieczeństwem informacji nie został precyzyjnie zdefiniowany przez właściciela systemu.

Polityka Bezpieczeństwa pl.ID, będąca jedną z podstaw zarządzania bezpieczeństwem SRP, w tym w COI, w większości obszarów zawiera jedynie cel oraz krótkie przedstawienie danego zagadnienia. Brakuje w niej szczegółowych informacji i wskazania konkretnych dokumentów zawierających odpowiednie procedury związane z tymi obszarami. W *Polityce Bezpieczeństwa pl.ID* brakuje zdefiniowanych procedur: komunikacji między COI a ministerstwem pełniącym funkcje zarządcze w zakresie SRP, zarządzania kontami użytkowników[43], nadawania i administrowania uprawnieniami; brakuje w pełni zdefiniowanej polityki zarządzania kontrolą dostępu do SRP, polityki bezpieczeństwa osobowego oraz systemu zarządzania ciągłością działania. W pkt. 6 *Polityki Bezpieczeństwa pl.ID* podano, że zasady funkcjonowania Systemu Zarządzania Bezpieczeństwem Informacji określają odrębne dokumenty. Z informacji przekazanych przez Minister Cyfryzacji Panią Annę Streżyńską wynika, że powyższe dokumenty nie powstały z *Polityką Bezpieczeństwa pl.ID*. Ponadto, Minister Cyfryzacji poinformowała, że *dokumenty określające zasady funkcjonowania Systemu Zarządzania Bezpieczeństwem (SZBI) nie powstały jeszcze w MC. (…) prowadzone są prace związane z kształtem i treścią SZBI. (…) w przygotowaniu jest natomiast aktualizacja samej Polityki Bezpieczeństwa.*

(dowód: akta kontroli str. 1284-1427, 3338-3351, 3824-3834, 4321-4345, 4376-4516, 4527-4547, 4665-4671, 4683-4875)

3.2. Polityka bezpieczeństwa COI

Opis stanu faktycznego

Poza *Polityką Bezpieczeństwa pl.ID* ustanowioną przez MSW, COI realizował zarządzanie bezpieczeństwem SRP na podstawie *Polityki Bezpieczeństwa Informacji Centralnego Ośrodka Informatyki*, wprowadzonej zarządzeniem Nr 63/2015 Dyrektora COI z dnia 26 października 2015 r. Integralną częścią tej *Polityki* była m.in. procedura zgłaszania incydentu bezpieczeństwa. Dyrektor COI Pan Rafał Leśkiewicz poinformował, że *polityka jest sukcesywnie wdrażana. Trwają prace przygotowawcze związane z wdrożeniem w organizacji normy ISO 27001,*

[42] Dokument z dnia 24 lutego 2015 r.

[43] Zarządzanie kontami użytkowników zostało opisane w *Podręczniku Administratora Aplikacji Źródło*, *Dokumentacji Użytkownika Aplikacji Źródło – Podręcznik dla MSW* oraz w *Podręczniku Administratora Aplikacji Źródło – Administrator Lokalny*, jednakże wymienione podręczniki nie stanowią dokumentacji procesu zarządzania kontami użytkowników. Są to instrukcje użytkownika dla administratorów systemu Źródło.

w ramach której zostanie dokonana analiza (kontrola) istniejącego systemu bezpieczeństwa informacji. Harmonogram działań związanych z wdrożeniem ISO 27001 jest w trakcie ustalania.

(dowód: akta kontroli str. 1284-1427, 2193-2210, 2907-2921, 3384-3406, 3824-3834, 4704-4875)

3.3. Zarządzanie incydentami bezpieczeństwa

Opis stanu faktycznego

W okresie od 1 marca 2015 r. do 15 czerwca 2016 r. COI odnotował 142 zgłoszenia podejrzenia incydentów bezpieczeństwa. Część potwierdzonych incydentów bezpieczeństwa dotyczyła podłączenia stacji komputerowej wykorzystującej aplikację „Źródło" do publicznej sieci Internet. Dyrektor Pionu Bezpieczeństwa COI Pan Maciej Wardaszko wyjaśnił, że *wszystkie incydenty z zakresu bezpieczeństwa są sygnalizowane MC, w sposób zgodny z Polityką Bezpieczeństwa pl.ID*.

Kierownik Zespołu Administratorów Systemów z COI, Pan Grzegorz Grabowski potwierdził, że *zdarzało się, że komputer korzystając z systemu był jednocześnie podłączony do Internetu. Jest to poza gestią zarówno COI jak i MC, można tylko poinformować gminę o zakazie.*

Ponadto, Kierownik Zespołu Produkcji Oprogramowania II z COI, Pan Teodor Buchner poinformował, że *z inicjatywy COI opracowano narzędzie służące do sprawdzania czy stacja jest podłączona do sieci publicznej.* Dyrektor COI Pan Rafał Leśkiewicz wskazał, że *narzędzie zostało uruchomione pilotażowo na okres 1 tygodnia: 22-29.04.2016, żeby zweryfikować poprawność jego działania w środowisku produkcyjnym.*

Z ustaleń kontroli wynika, że obsada zespołu zajmującego się bezpieczeństwem IT w COI jest wystarczająca do zarządzania bezpieczeństwem SRP.

(dowód: akta kontroli str. 1284-1427, 1587-1588, 1977-1983, 2193-2210, 2570-2574, 2888-2889, 2907-2921, 3384-3406, 3824-3834, 3872-3879, 3997-4000, 4527-4547, 4704-4875)

3.4. Zapewnienie rozliczalności działań podejmowanych przez użytkowników SRP

Opis stanu faktycznego

Wszystkie operacje wykonywane w SRP są zapisywane przez opracowany przez COI podsystem „Audyt". Funkcjonują następujące rejestry służące do audytu systemu:

- rejestr udostępnień, który przechowuje informacje o wszystkich wchodzących do systemu żądaniach udostępnienia danych. Zawiera takie informacje jak: podmiot żądający dostępu, wszystkie parametry żądania, datę i czas żądania, czy dane i w jakim zakresie zostały udostępnione. W dokumencie *Architektura Systemu Rejestrów Państwowych* wskazano, że rejestr udostępnień jest przystosowany do odnotowywania informacji wskazanych w § 7 ust. 1 pkt 4 rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych[44];

[44] Dz. U. Nr 100, poz. 1024.

- rejestr zmian, który przechowuje informacje o tym jakie informacje zostały zmodyfikowane. Zawiera informacje takie jak: podmiot zmieniający dane, przedmiot zmiany, rodzaj zmiany, dane definiujące zmianę, datę i czas zmiany, czas realizacji żądania;
- rejestr podpisów (funkcjonuje podobnie do rejestru zmian).

(dowód: akta kontroli str. 1576-1579, 1701-1718)

3.5. Uprawnienia pracowników COI do pracy w SRP

Opis stanu faktycznego

W wyniku badania przeprowadzonego na próbie 10 pracowników COI wykonujących zadania w SRP stwierdzono, że zgodnie z § 20 ust. 2 pkt 4 rozporządzenia KRI, osoby te uczestniczyły w procesie przetwarzania informacji w stopniu adekwatnym do zadań wynikających z ich zakresów obowiązków. Ponadto ustalono, że dwie osoby posiadały konta dostępu do bazy danych w SRP pomimo zakończenia zatrudnienia w COI (szczegółowy opis w punkcie dotyczącym nieprawidłowości).

(dowód: akta kontroli str. 1284-1427, 1550-1568, 1825-1842, 3338-3351, 4344-4516)

W 2015 r. w COI przeprowadzono kontrolę wewnętrzną dotyczącą stosowania procedur w zakresie zabezpieczania komputerów przenośnych i ich użytkowania oraz przydzielania uprawnień administratora użytkownikom systemów teleinformatycznych. Badaniem objęto okres od 1 stycznia 2014 r. do 30 czerwca 2015 r. W wyniku kontroli nie sformułowano zaleceń w zakresie SRP.

(dowód: akta kontroli str. 4, 1499-1544)

3.6. Audyty i testy bezpieczeństwa SRP

Opis stanu faktycznego

W trakcie wytwarzania SRP były przeprowadzone[45], przez podmioty zewnętrzne, audyty i testy bezpieczeństwa systemu. Audytem objęto jakość kodu źródłowego i odporność systemu na ataki z zewnątrz. W przypadku stwierdzenia podatności systemu wdrożono odpowiednie poprawki oraz przeprowadzono powtórne audyty i testy bezpieczeństwa.

(dowód: akta kontroli str. 4, 1569-1579, 1977-2070, 3824-3834, 3872-4316, 4321-4345, 4527-4571, 4704-4875)

Uwagi dotyczące badanej działalności

NIK zauważa, że audyty i testy bezpieczeństwa przeprowadzane były jedynie w trakcie wytwarzania i wdrażania SRP i od chwili jego uruchomienia (czyli prawie półtora roku), pomimo wprowadzenia licznych zmian w systemie, nie został przeprowadzony żaden audyt/test bezpieczeństwa SRP.

Dyrektor Pionu Bezpieczeństwa COI Pan Maciej Wardaszko wyjaśnił, że testy bezpieczeństwa SRP są planowane na III/IV kwartał 2016 r. *Trwają ustalenia z Ministerstwem Cyfryzacji co do terminu i zakresu testów bezpieczeństwa*.

(dowód: akta kontroli str. 4, 1569-1579, 1977-2070, 3824-3834, 3872-4316, 4321-4345, 4527-4571, 4704-4875)

[45] W okresie od lipca 2014 r. do stycznia 2015 r.

3.7. Wykonywanie kopii zapasowych

Opis stanu faktycznego

Polityka wykonywania kopii zapasowych została opisana w dokumencie *Procedury eksploatacyjne SRP*, w pkt. 5. *System backupu/polityka backupów*. Polityka ta przewiduje, że *na wszystkich serwerach raz dziennie wykonywane są przyrostowe backupy wybranych filesystemów. Pełny backup baz danych Oracle jest wykonywany 1 raz w tygodniu, a backupy archivelog'ów wykonują się co 10 minut dla serwerów DB i co 20 minut dla serwerów LOG*. Na podstawie analizy logów kopii zapasowych ustalono, że kopie te były wykonywane przez COI zgodnie z procedurami.

(dowód: akta kontroli str. 1822-1823, 1966-1968, 4704-4875)

Ustalone nieprawidłowości

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

Dwie osoby, mimo zakończenia zatrudnienia w COI[46], posiadały niezablokowane konta z dostępem do bazy danych SRP. Było to niezgodne z § 20 ust. 2 pkt 5 rozporządzenia KRI, stanowiącym że zarządzanie bezpieczeństwem informacji realizowane jest w szczególności poprzez bezzwłoczną zmianę uprawnień w przypadku zmiany zadań osób zaangażowanych w proces przetwarzania informacji, a także z pkt. A.9.2.6 załącznika A normy PN-ISO/IEC 27001:2014-12, stanowiącym, że przydzielone pracownikom prawa dostępu do informacji i środków przetwarzania informacji należy odbierać po zakończeniu zatrudnienia.

Powyższe było niezgodnie także z pkt. 9.5 tiret 7 *Polityki Bezpieczeństwa Informacji Centralnego Ośrodka Informatyki*, stanowiącej że prawa dostępu pracowników oraz osób/podmiotów świadczących usługi na rzecz COI po zakończeniu zatrudnienia lub obowiązywania właściwej umowy są odbierane lub dostosowywane do zaistniałych zmian. Ponadto, w pkt. 2.4 procedury nr PB008 „Zasady nadawania, usuwania i modyfikacji uprawnień", będącej uzupełnieniem ww. Polityki Bezpieczeństwa COI, podano, że w przypadku gdy zachodzi konieczność usunięcia, bądź modyfikacji nadanych użytkownikowi uprawnień wniosek o usunięcie/modyfikację uprawnień składa kierownik komórki organizacyjnej użytkownika do administratora systemu.

W trakcie kontroli ww. konta zostały zablokowane 14 lipca 2016 r., tj. po 257 i 44 dniach od zakończenia przez pracowników zatrudnienia.

Dyrektor COI Pan Rafał Leśkiewicz wyjaśnił, że konta nie zostały zablokowane *w związku z zakłóceniami w przepływie informacji dotyczących ruchów kadrowych w COI. (…) Pragniemy podkreślić, że pomimo niezablokowanego konta, użytkownik nie mógł zalogować się do bazy ze względu na brak fizycznego dostępu. Dostęp jest możliwy tylko w wydzielonej strefie, z wydzielonej stacji roboczej i tyko z wydzielonej sieci. Aby dostać się do wydzielonych pomieszczeń użytkownik musi być pracownikiem COI i/lub posiadać kartę umożliwiającą dostęp do wydzielonych pomieszczeń. Karty takie są oddawane przez pracowników rozwiązujących umowę o pracę w ramach procesu rozliczania się z pracodawcą. W przypadku przebywania w strefie jako „gość" dostęp jest możliwy tylko w asyście pracownika COI.* Dyrektor COI poinformował, że nie odnotowano logowania na opisanych kontach byłych pracowników po zakończeniu przez nich zatrudnienia.

(dowód: akta kontroli str. 1284-1427, 1550-1568, 1825-1836, 2193-2210, 2575-2576, 4346-4516)

[46] Zakończenie zatrudnienia nastąpiło odpowiednio z dniem 31 października 2015 r. i 31 maja 2016 r.

Ocena cząstkowa

W ocenie NIK, COI podejmował działania w celu zapewnienia bezpieczeństwa SRP w zakresie mu powierzonym, a przyjęte w COI rozwiązania były adekwatne do potrzeb i spełniały swoją funkcję. *Polityka Bezpieczeństwa Informacji Centralnego Ośrodka Informatyki* spełnia obecnie obowiązujące standardy w zakresie zarządzania bezpieczeństwem informacji i jest właściwa zarówno w świetle dobrych praktyk, jak i pragmatyki. Polityka wymienia i opisuje procedury stosowane przez COI we wszystkich obszarach mających wpływ na bezpieczeństwo informacji w organizacji zdefiniowanych przez normę ISO 27001. COI podjęło działania w celu wdrożenia normy ISO/IEC 27001.

NIK zauważa, że trudność organizacji zapewnienia bezpieczeństwa SRP jako całości wynika z umiejscowienia infrastruktury systemu:

- serwerownie będące we władaniu MSWiA i Policji,
- sieć OST 112, której operatorem jest Policja nadzorowana przez MSWiA,
- komputery użytkowników końcowych zarządzane m.in. przez urzędy miast i gmin,
- infrastruktura obliczeniowa (serwery, macierze dyskowe, urządzenia kopii zapasowych) we władaniu COI,

co powoduje rozproszenie zadań/obowiązków w zakresie zapewnienia bezpieczeństwa SRP pomiędzy MC, COI, administrację rządową i samorządową, przy czym obowiązki każdej ze stron w tym zakresie nie są jednoznacznie określone.

W opinii NIK, organizacja zarzadzania bezpieczeństwem SRP powinna być w głównej mierze ustanowiona przez właściciela systemu, czyli Ministra Cyfryzacji. MSW wprowadziło wprawdzie w 2015 r. *Politykę Bezpieczeństwa pl.ID,* jednak nie określiło zasad funkcjonowania Systemu Zarządzania Bezpieczeństwem Informacji. Na dzień zakończenia kontroli zasady te nie zostały opisane i wdrożone przez właściciela SRP (Ministra Cyfryzacji). Wskazać przy tym należy, że obowiązująca *Polityka Bezpieczeństwa pl.ID* opracowana jeszcze przez MSW nie zawiera szczegółowych procedur umożliwiających sprawne zarządzanie bezpieczeństwem informacji SRP.

Dotychczasowy sposób zarządzania bezpieczeństwem informacji skutkuje tym, że kwestie bezpieczeństwa SRP nie są traktowane w sposób systematyczny, w ramach jasno zdefiniowanego, jednolitego podejścia zgodnego z dobrą, ustandaryzowaną praktyką zawartą w normie ISO 27001.

W opinii NIK, COI podejmował działania w celu sprawnego zarządzania incydentami bezpieczeństwa, m.in. poprzez opracowanie narzędzia informującego o dostępie stacji roboczej z aplikacją „Źródło" do publicznej sieci Internet.

COI zapewnił odpowiednie mechanizmy kontrolne w ramach SRP, pozwalające na stwierdzenie kiedy i do jakich danych urzędnik uzyskał dostęp, a także ocenę zasadności wglądu do bazy danych o obywatelach.

Stwierdzona w COI nieprawidłowość polegająca na nieodebraniu uprawnień dostępu do bazy danych SRP dwóm byłym pracownikom została usunięta w trakcie kontroli.

IV. Wnioski

Wnioski pokontrolne

W związku z usunięciem nieprawidłowości w trakcie kontroli, NIK odstępuje od sformułowania wniosku pokontrolnego.

V. Pozostałe informacje i pouczenia

Prawo zgłoszenia zastrzeżeń

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

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

Obowiązek poinformowania NIK o sposobie wykorzystania uwag

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 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.

Warszawa, dnia października 2016 r.

Najwyższa Izba Kontroli
Departament Administracji Publicznej

Kontrolerzy:
Agnieszka Klimowicz
główny specjalista k.p.

.....
podpis

Dyrektor
Bogdan Skwarka

.....
podpis

Bartosz Tajer
główny specjalista k.p.

.....
podpis

Piotr Bielecki
specjalista k.p.

.....
podpis