

VIII kadencja



KANCELARIA SEJMU

Biuro Komisji Sejmowych

PEŁNY ZAPIS PRZEBIEGU POSIEDZENIA

- **KOMISJI DO SPRAW
KONTROLI PAŃSTWOWEJ
(NR 52)
z dnia 8 czerwca 2017 r.**

Pełny zapis przebiegu posiedzenia

Komisji do Spraw Kontroli Państwowej (nr 52)

8 czerwca 2017 r.

Komisja do Spraw Kontroli Państwowej, obradująca pod przewodnictwem posła **Tadeusza Dziuby (PiS)**, zastępcy przewodniczącego Komisji, rozpatrzyła:

- informację Najwyższej Izby Kontroli o wynikach kontroli Systemu Rejestrów Państwowych – bezpieczeństwo, funkcjonowanie i użyteczność,
- sprawy bieżące.

W posiedzeniu udział wzięli: **Karol Okoński** podsekretarz stanu w Ministerstwie Cyfryzacji wraz ze współpracownikami, **Mieczysław Łuczak** wiceprezes Najwyższej Izby Kontroli wraz ze współpracownikami, **Dariusz Gawryś** dyrektor Pionu ds. Rozwoju Oprogramowania i Utrzymania Systemów w Centralnym Ośrodku Informatyki wraz ze współpracownikami, **Agnieszka Bolesta** dyrektor w Centrum Personalizacji Dokumentów w Ministerstwie Spraw Wewnętrznych i Administracji wraz ze współpracownikami.

W posiedzeniu udział wzięli pracownicy Kancelarii Sejmu: **Tadeusz Oset, Tadeusz Cieśluk** – z sekretariatu Komisji w Biurze Komisji Sejmowych.

Przewodniczący poseł **Tadeusz Dziuba (PiS):**

Dzień dobry. Otwieram posiedzenie Komisji do Spraw Kontroli Państwowej. Czy są uwagi do porządku dziennego? Nie słyszę. Stwierdzam, że porządek dzienny został przyjęty. Punkt pierwszy to informacja Najwyższej Izby Kontroli o wynikach kontroli Systemu Rejestrów Państwowych – bezpieczeństwo, funkcjonowanie i użyteczność. Witam wszystkich obecnych gości, pana prezesa Łuczaka i pana ministra Karola Okońskiego wraz z towarzyszącymi osobami. Proszę pana prezesa o zainaugurowanie naszej dyskusji. Ewentualnie, może później przekazać głos swoim współpracownikom. Zapraszam.

Wiceprezes Najwyższej Izby Kontroli **Mieczysław Łuczak:**

Panie przewodniczący, panie i panowie posłowie, panie ministrze, dziękuję za zaproszenie i możliwość przedstawienia wyników kontroli dotyczącej Systemu Rejestrów Państwowych. Kontrola stanowi kontynuację szeregu działań podejmowanych przez NIK, dotyczących informatyzacji państwa. W ostatnich latach NIK przeprowadziła m.in. kontrolę świadczenia usług publicznych w formie elektronicznej, na przykładzie wybranych jednostek samorządu terytorialnego. Następną kontrolą dotyczyła wdrażania wybranych wymagań dotyczących systemów teleinformatycznych, wymiany informacji w postaci elektronicznej oraz krajowych ram interoperacyjności oraz realizacji przez podmioty państwowe zadań w zakresie ochrony cyberprzestrzeni. NIK skontrolowała i oceniła nowy, informatyczny system rejestrów państwowych pod kątem funkcjonalności i zapewnienia bezpieczeństwa danych oraz poprawy obsługi obywateli. Kontrolę prowadzono w 2016 r. w 14 jednostkach, tj. Centralnym Ośrodku Informatyki oraz 13 wybranych urzędach miast i gmin w województwach: dolnośląskim, mazowieckim, podkarpackim i podlaskim. Ponadto, uzyskano dodatkowe informacje z Ministerstwa Cyfryzacji oraz Ministerstwa Spraw Wewnętrznych i Administracji. Badaniami objęto okres od 1 stycznia 2013 r. do 31 lipca 2016 r. Warto wspomnieć, że z dniem 1 marca 2015 r. lokalne systemy informatyczne w urzędach miast i gmin, wykorzystywane m.in. do obsługi spraw z zakresu stanu cywilnego i ewidencji ludności, zastąpiono jednym, ogólnokrajowym, elektronicznym Systemem Rejestrów Państwowych. System to centralny rejestr państwa, który łączy najważniejsze ewidencje, m.in. rejestry: PESEL, dowodów osobistych, stanu cywilnego. System Rejestrów Państwowych wykorzystywany jest przez urzędy

gmin i stanu cywilnego do załatwiania spraw dotyczących m.in.: dowodów osobistych, meldunków, aktów stanu cywilnego, aktów urodzenia, małżeństwa, zgonu i innych dokumentów. Do wykorzystania Systemu Rejestrów Państwowych służy urzędnikom aplikacja „Źródło”. Integracja rejestrów państwowych w systemie była jednym z celów stworzenia programów identyfikacji, zarządzanego od 2013 r. przez ministra spraw wewnętrznych i administracji. Na wykonanie systemu rejestrów państwowych wydatkowano 109 mln zł, a jego utrzymanie do czerwca 2019 r. będzie kosztować kolejne 97 mln zł. Pozytywnie należy ocenić, że dane, udostępnione w SRP z dniem 1 marca 2015 r., umożliwiły obywatelom załatwienie spraw dotyczących dowodów osobistych i wydawania odpisów aktów stanu cywilnego w dowolnym urzędzie gminy, niezależnie od miejsca zamieszkania. Wraz z uruchomieniem SRP, udostępniono 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. Następnie umożliwiono złożenie przez Internet wniosku o wydanie dowodu osobistego i odpisu aktu stanu cywilnego oraz zgłoszenie utraty dowodu osobistego. Kontrola NIK wykazała, że przygotowanie i udostępnienie SRP obarczone było jednak wieloma błędami po stronie ówczesnych: Ministerstwa Spraw Wewnętrznych i Administracji, zlecającego budowę SRP, oraz Centralnego Ośrodka Informatyki, jako wykonawcy, co spowodowało, iż w trakcie użytkowania systemu wystąpiły utrudnienia dla obywateli i urzędów korzystających z SRP. System uruchomiono z dwumiesięcznym opóźnieniem, a po jego udostępnieniu ujawniono wiele usterek, także braki funkcjonalności aplikacji „Źródło”, wykorzystywanej do obsługi SRP w urzędach. Użytkownicy aplikacji „Źródło” zwracali uwagę na potrzebę ułatwienia obsługi załatwiania spraw z wykorzystaniem tego programu. Przykładowo, wydanie takiego samego odpisu aktu stanu cywilnego wymagało wielokrotnego powtarzania tych samych czynności w aplikacji, co wydłużało obsługę. Ponadto, po wdrożeniu SRP w kontrolowanych urzędach wystąpiły opóźnienia w wydawaniu obywatelom odpisów aktów stanu cywilnego. Główną przyczyną opóźnień było niezapewnienie przez ówczesne MSWiA i COI, na etapie przygotowania systemu, przeniesienia aktów stanu cywilnego, zgromadzonych dotychczas w lokalnych bazach danych, do rejestru stanu cywilnego w SRP. Spowodowało to konieczność przenoszenia pojedynczych danych aktów stanu cywilnego z lokalnych systemów do SRP w celu wydania odpisu lub wprowadzenia aktów do systemu z papierowej księgi stanu cywilnego. W wielu przypadkach zaniechanie to przyczyniło się do konieczności wielodniowego oczekiwania na wprowadzenie do systemu danych przez urząd zamiejscowy, zamiast wydania aktu na poczekaniu. Zaniechanie przyczyniło się także do wzrostu kosztów załatwiania spraw z zakresu stanu cywilnego, zwłaszcza w dużych miastach. W 54% zbadanych urzędów nastąpił wzrost zatrudnienia wśród osób zajmujących się sprawami stanu cywilnego (najwyższy w Urzędzie Miasta Stołecznego Warszawy, o 48 osób). Według szacunków gmin, pojedyncze przenoszenie aktów stanu cywilnego do SRP potrwałoby co najmniej kilka lat. Ministerstwo Cyfryzacji i Centralny Ośrodek Informatyki przystąpiły do opracowania rozwiązania, umożliwiającego zbiorcze przeniesienie danych z systemów lokalnych do SRP. Udostępnienie zostało zaplanowane na drugi kwartał bieżącego roku.

W opinii Najwyższej Izby Kontroli, problemy w przygotowaniu i działaniu Systemu Rejestrów Państwowych wynikały w szczególności z: nieuwzględnienia masowej migracji aktów stanu cywilnego z lokalnych systemów do SRP, co wpływało na opóźnienia w ich wydawaniu, odpisów i wzrost kosztów załatwiania spraw; błędów oprogramowania systemu (w związku z tym, system został odebrany i uruchomiony warunkowo po upływie dwóch miesięcy od pierwotnego planu oddania do użytku); braku decyzji ministra spraw wewnętrznych i administracji o wprowadzeniu wdrożenia pilotażowego, które pozwoliłoby na przetestowanie systemów w praktyce oraz wykrycie i usunięcie wad; zawarcie przez ministra cyfryzacji umowy na utrzymanie i rozwój SRP dopiero po ponad roku od udostępnienia systemu (utrudniało to wprowadzenie nowych, a także rozbudowę istniejących funkcjonalności, równoległe prowadzonych prac programistycznych przy budowie systemu i opracowania aktów prawnych w zakresie rejestracji stanu cywilnego); brak konsekwentnego zastosowania metodyk zarządzania programami przez ówczesne MSWiA oraz częstych zmian na stanowisku kierownika projektu.

Wprowadzenie SRP ujawniło liczne rozbieżności w danych o obywatelach zgromadzonych w rejestrach wchodzących w skład systemu. Dotyczyły one najczęściej: braku nazwiska rodowego wnioskodawcy, błędów w imionach, nazwiskach, miejscach urodzenia i danych rodziców, braku informacji o aktualnym stanie cywilnym, błędów w kodach pocztowych oraz braku serii, numeru i dat ważności ostatnio wydanego dowodu osobistego. NIK ocenia, że wdrożony już przez CIO system rejestrów państwowych oraz mechanizmy weryfikacji danych przyczyniają się do poprawy znajdujących się w rejestrach jakości. We wszystkich badanych przypadkach urzędy podejmowały działania mające na celu wyjaśnienie rozbieżności, a następnie usuwano je lub wysyłano zalecenia ich usunięcia do właściwych urzędów. Natomiast, nasz niepokój budzi fakt, że zarządzanie bezpieczeństwem Systemu Rejestru Państwowych, który zawiera bardzo istotne dane o obywatelach, jak imię, nazwisko, nr PESEL, adres zameldowania, stan cywilny, nie zostało kompleksowo zorganizowane i uregulowane. Opracowana przez ówczesne MSWiA polityka bezpieczeństwa systemu nie zawierała szczegółowych rozwiązań, które powinny zostać określone w odrębnych dokumentach. Dokumenty nie powstały. Nie zdefiniowano procedur komunikacji między CIO, a ministerstwem odnośnie do zarządzania kontami użytkowników, administrowania i nadawania uprawnień. Brakowało również w pełni zdefiniowanych polityk zarządzania kontrolą dostępu do systemu, a także procedur bezpieczeństwa osobowego oraz systemu zarządzania ciągłością działania. Ponadto, NIK zwróciła uwagę, że audyt i test bezpieczeństwa SRP prowadzone były jedynie w trakcie jego wytwarzania i wdrażania, natomiast przez prawie pół roku od jego uruchomienia nie przeprowadzono obowiązkowego, corocznego audytu bezpieczeństwa. Ministerstwo Cyfryzacji poinformowało, że prowadzi prace w wyżej wymienionym zakresie. Najwyższa Izba Kontroli zwracała także uwagę, że ustalony w umowie między ministrem cyfryzacji, a Centralnym Ośrodkiem Informatyki okres rozwiązywania i usuwania problemów, związanych z bieżącym funkcjonowaniem SRP, był zbyt długi.

Zgodnie z umową, w przypadku wystąpienia w systemie tzw. incydentu krytycznego, usuwanie awarii może trwać nawet trzy dni, co może oznaczać trzydniową przerwę w działaniu systemów w całym kraju, a w konsekwencji brak możliwości rejestracji w systemie narodzin, małżeństw lub zgonów. Pozytywnie należy ocenić, że COI należycie wywiązywał się z powierzonych zadań w zakresie monitorowania bezpieczeństwa systemu, zapewnienia bezpieczeństwa zmian oraz zarządzania incydentami bezpieczeństwa. Część z nich dotyczyła połączenia stacji komputerowych urzędów wykorzystujących aplikację „Źródło” z publiczną siecią Internet, pomimo, że MWSiA i COI wskazały, iż na stacjach komputerowych, pracujących w systemie, nie jest dozwolona konfiguracja, umożliwiająca nawiązywanie połączeń wchodzących do sieci Internet oraz zalecana jest pełna separacja od innych sieci. COI opracował narzędzia do sprawdzania, czy stacja jest podłączona do stacji publicznej. Problemem jest jednak brak narzędzi prawnych pozwalających na wyciąganie konsekwencji wobec użytkowników SRP. NIK stwierdziła, że kierownicy kontrolowanych urzędów miast nie przywiązywali na ogół dostatecznej wagi do zapewnienia bezpieczeństwa przetwarzania informacji z wykorzystaniem SRP. W 62% kontrolowanych urzędów nie opracowano i nie wdrożono polityk bezpieczeństwa informacji. W 23% badanych urzędów nie przestrzegano wymogu zablokowania dostępu do Internetu na komputerach wykorzystywanych do pracy w SRP. Kwestie te wymagają rozwiązania, gdyż z umożliwieniem dostępu do Internetu na komputerach z aplikacją „Źródło” wiąże się ryzyko wycieku zgromadzonych w SRP danych o obywatelach, dotyczących tak istotnych spraw jak: akty stanu cywilnego, dowody osobiste, numery PESEL oraz numery ewidencyjne. W 38 skontrolowanych urzędach wystąpiły nieprawidłowości w zakresie blokowania lub odbierania dostępu do aplikacji „Źródło” byłym pracownikom (osoba, która przestała pracować nadal miała dostęp do informacji). W 23% urzędów nie prowadzono obowiązkowego, corocznego audytu w zakresie bezpieczeństwa informacji w systemach informatycznych. Biorąc pod uwagę potrzebę wzmocnienia bezpieczeństwa, NIK przekazała drogą elektroniczną informację o wynikach kontroli wszystkim prezydentom miast, burmistrzom i wójtom. Po kontroli NIK wniosowała do ministra cyfryzacji o: opracowanie szczegółowych procedur w ramach polityki bezpieczeństwa, dotyczącej systemu rejestru państwowego; przeprowadzenie migracji danych dotyczą-

cych stanu cywilnego z lokalnych systemów informacji do systemu państwowego; zapewnienie usunięcia przez COI pozostawionych błędów w oprogramowaniu oraz poprawę funkcjonalności SRP pod kątem wymagań użytkowników; wypracowanie rozwiązań umożliwiających egzekwowanie od kierowników urzędów wymogu odseparowania stacji komputerowych z aplikacją „Źródło” od sieci komputerowych; podjęcie działań w celu zagwarantowania krótszych okresów usuwania awarii systemu, określonych w obowiązującej umowie z COI dotyczącej utrzymania systemu.

Po kontroli wnioskowaliśmy do burmistrzów i prezydentów miast o zapewnienie terminowego przenoszenia aktów stanu cywilnego do systemu na wnioski innych urzędów, w celu sprawnego załatwienia spraw obywateli, opracowania i wdrożenia polityki bezpieczeństwa informacji oraz wprowadzenia corocznego audytu bezpieczeństwa informacji, uniemożliwienia dostępu do Internetu na komputerach pracujących z SRP, niezwłocznego odebranie pracownikom uprawnień w chwili zakończenia zatrudnienia lub zmiany zakresu obowiązków. Ministerstwo Cyfryzacji razem z Centralnym Ośrodkiem Informatyki podjęło pracę nad usprawnieniem systemu, w tym dotyczącą funkcjonalności wykorzystywanych przez użytkowników. Podjęto również prace rozwojowe. Aktywne włączenie w prace użytkowników może pozytywnie wpłynąć na eliminowanie błędów i usprawnienie załatwiania spraw obywateli. Kierownicy kontrolowanych urzędów miast podjęli wnioski NIK do realizacji. Wyniki badania przeprowadzonego w 2016 r. przez Ministerstwo Cyfryzacji wskazują, że 61% Polaków chce przez Internet załatwić sprawy związane z wydawaniem lub wymianą dowodu osobistego, a 20% obywateli jest zainteresowanych rejestracją urodzenia dziecka lub dokonaniem meldunku tą drogą. Kwestie dotyczące funkcjonowania SRP są bardzo istotne nie tylko dla państwa, ale przede wszystkim dla obywateli.

Szanowni państwo, to wszystko z naszej strony. Jeżeli pojawią się pytania, jesteśmy do państwa dyspozycji. Dziękuję.

Przewodniczący poseł Tadeusz Dziuba (PiS):

Teraz oddam głos panu ministrowi, ale zastrzegam, że to co usłyszeliśmy, co można wyczytać w raporcie NIK, chociaż w formule urzędniczej, jest bardzo groźne. Czy pan minister może odnieść się do wyników kontroli, ale przede wszystkim w aspektach bezpieczeństwa SRP? Bardzo proszę.

Podsekretarz stanu w Ministerstwie Cyfryzacji Karol Okoński:

Panie przewodniczący, Wysoka Komisjo, panie prezesie, zgadzam się, że skomasowanie problemów w krótkim czasie oraz w prezentacji, pokazuje, iż liczba zagadnień wymagających wyjaśnienia jest duża. Natomiast, faktem jest, że ściśle współpracowaliśmy, równolegle do przygotowania raportu NIK i tuż po jego opracowaniu, aby wszystkie sprawy poprawić i wprowadzić w życie maksymalnie szybko. Dziękuję za wykonanie kontroli, była ona dla nas okazją, żeby w systematyczny sposób przyjrzeć się zagadnieniom wymagającym zmiany. Za chwilę odniosę się do aspektów bezpieczeństwa, o których mówił pan przewodniczący. Mamy sześć głównych wniosków wynikających z kontroli i chcę się do nich krótko ustosunkować.

Pierwsza wspomniana kwestia, z którą się zgadzamy, to niedopatrzenie, że w pierwotnym zakresie projektu nie było uwzględnionej migracji stanu cywilnego. Niezwłocznie po zdiagnozowaniu sytuacji, kiedy Ministerstwo Cyfryzacji przejęło rolę ministerstwa nadzorującego ten projekt, przystąpiliśmy do przygotowania rozwiązania, które umożliwiłoby przyspieszenie procesu i rozpoczęcie tzw. masowej migracji stanu cywilnego. Zgodnie z przekazanymi wcześniej informacjami, prace są na ukończeniu. Zakładam, że jeszcze w tym miesiącu będziemy w stanie uruchomić produkcyjnie funkcjonalność, która pozwoli przyspieszyć migrację. W ramach pilotażu z miastami Częstochowa i Nowa Sól będziemy testowali, czy rozwiązanie jest stabilne i spełnia oczekiwania użytkowników. Zakładam, że to jest dodatkowy wentyl bezpieczeństwa, dlatego, iż rozwiązanie powstawało już z użytkownikami, producentami tych aplikacji, które obecnie znajdują się w urzędach i obsługują lokalne bazy. Jednak uważamy, że okres pilotażu pozwala w bezpieczny sposób podejść do masowego wdrożenia, aby uniknąć sytuacji, iż wprowadzamy narzędzie obowiązujące we wszystkich urzędach, mogące generować problemy. Uwa-

zamy, że okres pilotażu potrwa do października i od listopada będziemy mogli masowo uruchomić funkcjonalność we wszystkich urzędach, w których pracownicy stanu cywilnego, oprócz swoich bieżących obowiązków, będą dokonywali procesu systematycznej migracji akt stanu cywilnego. Przykładamy też wagę do aspektów wydajnościowych, żeby prace nie miały wpływu na bieżące czynności w urzędach. Obecne wyniki testów wydajnościowych pozwalają sądzić, że można pogodzić dwa procesy bieżącej obsługi migracji. Zakładamy, iż przy obecnym tempie migracji, proces mógłby zakończyć się do końca przyszłego roku.

Drugi aspekt dotyczył generalnie podejścia do bezpieczeństwa w projekcie SRP. Trwają prace, żeby opracować całościową politykę bezpieczeństwa SRP, która uwzględniłaby wszystkie wspomniane aspekty. Zakładamy, że polityka będzie gotowa jeszcze w tym roku. Jest ona w trakcie przygotowywania, ale nie zmienia to faktu, iż z jednej strony zakładamy, że aplikacja „Zródło” jest obsługiwana na komputerach, które są odseparowane od sieci, a z drugiej strony, nie było to skutecznie kontrolowane. Równolegle, oprócz opracowania całościowej polityki, wdrożyliśmy narzędzie, pozwalające na bieżąco monitorować stacje robocze w zakresie dostępu do Internetu, żeby wyłapywać na bieżąco podobne przypadki i zgłaszać je do kierowników urzędów.

Jeśli chodzi o kwestię błędów oprogramowania, faktycznie, w momencie, kiedy wdrożenie zostało uruchomione, pomimo opóźnienia, wygenerowano wiele błędów różnych kategorii w liczbie 1000. W 2016 r. prace zmierzały do wyeliminowania błędów. Mogę powiedzieć, że z 1000 błędów obecnie zostało tylko 6 zgłoszeń, które są w trakcie analizy. Wszystkie pozostałe zostały wdrożone podczas produkcji albo oczekują na wdrożenie razem z masową migracją stanu cywilnego. Szczęśliwie, aspekt związany z poprawą błędów jest już na ukończeniu. Na bieżąco wszystkie nowe błędy są monitorowane i rozwiązywane. Chcę podkreślić, że błędy oczekujące naprawy oraz diagnoza wniosków o zmianę usprawnień nie odbywają się w zaciszu ministerstwa lub Centralnego Ośrodka Informatyki, ale są dyskutowane na forum z użytkownikami końcowymi w ramach grup roboczych, w skład których wchodzi przedstawiciele urzędów, wykorzystujący oprogramowanie w bieżącej pracy. Z nimi są podejmowane decyzje odnośnie do proponowanych rozwiązań, co jest przyjmowane pozytywnie. Kalendarz pracy grupy i dynamika pokazuje, że we wszystkich, kolejnych projektach będziemy chcieli utrzymać ten model.

Jeśli chodzi o skrócenie czasów naprawy błędów, proces obsługi zgłoszeń w obecnym momencie został poprawiony. Jeśli chodzi o obsługę zgłoszeń krytycznych, w bieżącym, 2017 r. mieliśmy tylko jeden podobny błąd, który został poprawiony w ciągu godziny. Muszę powiedzieć, że od strony praktycznej jest znacząca poprawa, natomiast od strony formalnej wciąż zastanawiamy się nad aneksowaniem umowy dotyczącej SRP, jednak wymaga to dodatkowej analizy. W tym procesie musimy również uwzględnić elementy związane z tzw. komponentem niejawnym, który z racji problemów natury technologicznej nakłada dodatkowe prace, wydłużając proces obsługi błędów. Jednak, będziemy zmierzać, żeby okresy obsługi błędów mogły zostać skrócone od strony formalnej.

Odnośnie do uwagi dotyczącej faktu, że projekt nie do końca był prowadzony zgodnie z najlepszymi praktykami zarządzania, muszę powiedzieć, iż w Ministerstwie Cyfryzacji powstało biuro i wdrożono metodykę zarządzania portfelem projektów. Objęła ona również projekt SRP, podzieliła różne poziomy zarządzania, strategii, tzw. komitetu sterującego, poziom kierowników projektów i liderów zespołu. Podobnie w COI, zostały także wykonane prace w celu uporządkowania tej sfery. Proces jest znacznie bardziej uporządkowany i systematyczny niż wcześniej.

Odnośnie do zaangażowania użytkowników końcowych, wspominałem, że są grupy robocze, które na bieżąco monitorują wszystkie nowe zgłoszenia i opiniują wnioski o zmianę priorytetów. Można powiedzieć, iż system jest obecnie rozwijany łącznie i wspólnie z użytkownikami końcowymi, co przekłada się na większy poziom satysfakcji i zadowolenia niż wcześniej. Wpływa również na zmianę diagnozy, postawionej w raporcie NIK, która w pełni zostanie zaadresowana w momencie zakończenia migracji stanu cywilnego i kiedy będzie wdrożona polityka bezpieczeństwa. Obie sprawy planowane są jeszcze w tym roku.

To wszystko tytułem uzupełnienia i wyjaśnienia. Jeśli pojawią się pytania, jesteśmy do dyspozycji.

Przewodniczący poseł Tadeusz Dziuba (PiS):

Czy przedstawiciele Ministerstwa Spraw Wewnętrznych i Administracji chcą dodać coś do wypowiedzi pana ministra? Proszę się przedstawić.

Zastępca dyrektora w Ministerstwie Spraw Wewnętrznych i Administracji Urszula Rudynek-Ciechomska:

Urszula Rudynek-Ciechomska, zastępca dyrektora Departamentu Spraw Obywatelskich, który zajmuje się zadaniami związanymi z merytorycznym nadzorem nad rejestracją stanu cywilnego. Nasza rola pozostała bez zmian, natomiast wszelkie zadania projektowe zostały przeniesione do Ministerstwa Cyfryzacji. Mogę tylko dodać, że cały czas współpracujemy z Ministerstwem Cyfryzacji, bierzemy udział w pracach grupy roboczej, jak również komitetu sterującego, aby współpraca była pełna i zadania z zakresu rejestracji stanu cywilnego, nie tylko od strony projektowej, ale również merytorycznej, mogły być jak najlepiej i w pełni realizowane na bieżąco. Dziękuję.

Przewodniczący poseł Tadeusz Dziuba (PiS):

Panie i panowie posłowie, zapraszam do pytań. Pani przewodnicząca.

Poseł Barbara Chrobak (Kukiz15):

Panie przewodniczący, szanowna Komisjo, mam pytanie do przedstawiciela Ministerstwa Spraw Wewnętrznych i Administracji. W raporcie czytamy, że siedmiokrotnie nastąpiła zmiana na stanowisku kierownika, odnośnie do realizacji programu pl.ID. Czy państwo wiedzą, co było przyczyną częstej zmiany i jak długo obecny kierownik jest na tym stanowisku?

Poseł Kazimierz Moskał (PiS):

Panie przewodniczący, Wysoka Komisjo, panie ministrze, panie prezesie. Temat jest bardzo ważny i istotny. Każde państwo chce funkcjonować w sposób sprawny. System Rejestrów Państwowych ma temu służyć. Mamy problem użyteczności i funkcjonowania systemu, ale również bezpieczeństwa obywatela. Mam w tym kontekście pytania do pana prezesa i pana ministra. Pan prezes powiedział, że istnieje problem z aplikacją „Źródło” i ludźmi, którzy mieli do niej dostęp i mogli nadal wykorzystywać dane, kiedy już nie pracowali. Czy zdarzyło się, aby osoby pozbawione uprawnień, w jakikolwiek sposób wykorzystywały gromadzone dane? Mam ogólne pytanie do pana ministra cyfryzacji. System zawiera ogromną wiedzę, którą można różnie wykorzystać. Ma być ona użyteczna dla społeczeństwa, ale ktoś może sięgać po te źródła w nieodpowiedni sposób. Czy zdarzyły się osoby lub instytucje, które próbowały w sposób nieuprawniony sięgać do źródeł będących w dyspozycji ministerstwa? Czy i na jakim poziomie dochodzi ewentualnie do włamań i wykorzystywania danych w sposób nieuprawniony? Dziękuję.

Poseł Ryszard Wilczyński (PO):

Uzyskaliśmy obraz fazy budowania rejestrów państwowych, wychodzenia z bałaganu, rozproszenia systemów lokalnych, kupowanych przez gminy od różnych użytkowników, spinanych przez wojewodów. Gdyby wzorowano się na budowie autostrady, czyli na końcu przychodzi odbiór techniczny i wszystko musi działać od razu, system ten nigdy by nie powstał. Został on zbudowany na zasadzie: rozpoznać podczas boju – dana firma, potrafiąca zbudować oprogramowanie, zaczyna uruchamiać system, pojawiają się tysiące błędów, które korygujemy, współpracujemy z wojewodami i wydziałami spraw obywatelskich. Mam następujące pytanie: czy obecnie mamy model, jak powinno przebiegać opracowanie i wdrożenie lub integracja systemu państwowego? Istnieje CEPiK – gigantyczna baza, która nie jest z tym zintegrowana. Wyobraźmy sobie, że policjant zatrzymując samochód na drodze, wchodzi do systemu, dowiaduje się wszystko o obywatelu – czy jest kierowcą, posiada samochód i wystawia elektroniczny mandat. Mamy jeszcze wiele spraw do zrobienia.

Druga kwestia, czy państwo przeanalizowali zasoby, które były pozostawione do dyspozycji? Sytuacja końcowego użytkownika pokazuje, że nie. System jest całkowicie

państwowy, łącznie z urzędnikiem, który go obsługuje, komputerem, miejscem pracy, wszystkimi procedurami oraz przeszkoleniem. Mamy do czynienia z silnymi gminami, np. w Warszawie, i słabymi, np. Dubicze Cerkiewne. To są kompletnie różne światy. Człowiek, który tam pracuje ma często dziesiątki zadań, a na końcu dostaje do wdrożenia program pl.ID. Nie wyobrażam sobie, że w przyszłości będziemy pracowali na zasadzie: „weźta się i zróbcie”. To jest metoda typu: „wojewodo, spróbuj dopchnąć kolanem”. Ta faza musi odejść, nie może się już zdarzać. Chcę się dowiedzieć, czy mamy model i czy zostały zebrane stosowne zasoby, aby wdrożenie przebiegało u końcowego użytkownika właściwie?

Na koniec zadam pytanie o rolę Ministerstwa Cyfryzacji. Zawsze dochodzi do kłótni, kto jest właścicielem systemu? Użytkownicy, właściciele systemu starają się wszystko ogarnąć i nagle pojawiają się przedstawiciele Ministerstwa Cyfryzacji. Czy obecnie został wypracowany model, np. kto będzie integrował system z CEPiK-iem? Jaka będzie rola Ministerstwa Cyfryzacji? Czy będziecie jedynie klientem w MSWiA? Pytania są ważne na przyszłość.

Przewodniczący poseł Tadeusz Dziuba (PiS):

Dziękuję. Zostały zadane trzy pytania, poproszę o odpowiedzi, ale w odwrotnej kolejności – najpierw przedstawiciela MSWiA, następnie pana ministra, a na koniec pana prezesa.

Zastępca dyrektora w MSWiA Urszula Rudynek-Ciechomska:

Szanowni państwo, odniosę się do kwestii kierownika projektu, gdyż pytanie było kierowane do MSWiA. Chcę tylko powiedzieć, że sprawy związane z powoływaniem kierowników projektów należą do struktur zarządczych pl.ID i nie leżą obecnie w gestii ministra spraw wewnętrznych i administracji. To są zadania przeniesione do Ministerstwa Cyfryzacji w ramach podziału, który dokonał się z końcem 2015 r. Natomiast, z punktu widzenia nadzoru nad merytorycznymi zadaniami, zmiany, które miały miejsce, też nie były korzystne. Lepiej, gdyby był jeden kierownik i została zachowana ciągłość zarządzania projektem. To są kwestie zarządcze, a nie merytoryczne związane z realizacją zadań stanu cywilnego. Dziękuję.

Podsekretarz stanu w MC Karol Okoński:

Panie przewodniczący, Wysoka Komisjo, odnośnie do pierwszego pytania dotyczącego kierownika projektu, sytuacja jest stabilna. W COI jest kierownik projektu, który zajmuje się tymi sprawami od prawie roku. Po stronie Ministerstwa Cyfryzacji pracuje również osoba, która opiekuje się tym od roku. Jednocześnie, od kilku miesięcy mamy dedykowaną do projektu SRP osobę w randze zastępcy dyrektora Departamentu Utrzymania Rozwoju Systemów. Zatem, stabilność i ciągłość informacji, słusznie podniesiona, jako jedna z ważnych kwestii, w tym przypadku projektu SRP, w obecnej sytuacji jest utrzymana. Sytuacja dotycząca częstej wymiany, opisana w raporcie NIK-u, nie ma już miejsca.

Jeśli chodzi o pytanie pana posła Moskala, czy w raporcie NIK-u zostały stwierdzone wykroczenia wynikające z faktu nieuprawnionego dostępu, odpowiedź pozostawię panu prezesowi NIK. Natomiast, w kwestii pytania, czy obecnie były przypadki nieuprawnionego dostępu lub włamania do systemu SRP, oddam głos panu dyrektorowi Gawrysiowi, który odpowiada za rozwój i utrzymanie systemu w COI.

Dyrektor Pionu ds. Rozwoju Oprogramowania i Utrzymania Systemów w Centralnym Ośrodku Informatyki Dariusz Gawryś:

Panie przewodniczący, panie prezesie, szanowni państwo, jestem dyrektorem Pionu ds. Rozwoju Oprogramowania i Utrzymania Systemów w COI i odpowiadam za rozwój oprogramowania, które tworzone jest na zlecenie ministerstwa oraz utrzymane później w ramach zleceń na umowy utrzymaniowe i umowy zarządzania systemami. Dla przypomnienia powiem, że zarówno rozwój, leżący w gestii ministerstwa, jak i utrzymanie systemu są realizowane na zlecenie Centralnego Ośrodka Informatyki. System jest zainstalowany w naszych serwerowniach i użytkownicy mają dostęp poprzez sieć SRP. Odpowiadając na pytanie odnośnie do włamań, nieuprawnionego dostępu lub wycieku danych, system jest tak zbudowany, że każda operacja, dokonana przez jakiegokolwiek

użytkownika, jest podwójnie zapisywana w specjalnym, drugim systemie. Zatem, w każdej chwili możemy odtworzyć działanie użytkownika wstecz od samego początku działania. Drugi system jest poza zasięgiem operatorów i osób, które próbowałyby go zmienić. Jest nienaruszalny, jego integralność jest podstawą działania systemu. Dzięki temu, możemy sprawdzić, kto się logował i jaką operację wykonał w systemie. Jest on zabezpieczony w sposób, aby nie można wykonywać w nim żadnych operacji spoza systemu, wyłącznie przy pomocy aplikacji „Źródło”, który służy wszystkim urzędnikom i pracownikom, korzystającym z systemu, do wprowadzania zmian, wydawania aktów i prowadzenia obsługi obywateli. Istnieją jedynie dwa wydzielone miejsca, będące pod pełną kontrolą, w których takie operacje są realizowane pod nadzorem i wyłącznie za zgodą Ministerstwa Cyfryzacji. Mają one związek z jakością danych, co zostało wskazane w raporcie. Niestety, istnieją przypadki, że jakość danych jest bardzo słaba, ale cały czas pracujemy nad poprawą. Dzięki tym mechanizmom nie ma możliwości wykonania nieautoryzowanej operacji w systemie. Zapewne słyszeli państwo o przypadku pobrania dużej ilości danych przez urzędy komornicze. To była sytuacja dopuszczona prawem, czyli zgodnie z regulacjami, komornicy mają dostęp do aplikacji „Źródło” i danych PESEL. Nasze systemy bezpieczeństwa wykryły nienormalny ruch w czasie pobierania danych z systemu PESEL przez uprawnione podmioty. Zostało to zgłoszone i obecnie jest prowadzone postępowanie przez Agencję Bezpieczeństwa Wewnętrznego oraz odpowiednie organy, w celu wyjaśnienia, dlaczego komornicy dokonali pobrania na tak dużą skalę? Pełen system zabezpieczeń, samo-odseparowanie systemu od sieci dostępnych publicznie stanowi podstawę bezpieczeństwa systemu. Zwracamy uwagę, testujemy i sprawdzamy, czy punkty wykorzystywane jako stacje dostępu do aplikacji „Źródło”, nie są również połączone z innymi sieciami, zwłaszcza z internetem. To jest nasze codzienne działanie. W zeszłym roku w Centralnym Ośrodku Informatyki został powołany zespół bezpieczeństwa technicznego, którego zadaniem jest 24-godzinne monitorowanie bezpieczeństwa operacji w Systemach Rejestrów Państwowych. Dziękuję.

Wiceprezes NIK Mieczysław Łuczak:

Dziękuję, panie przewodniczący. Zapewne państwo podsumują, że na pierwsze pytanie została już udzielona odpowiedź i to działanie nie należy do naszej kompetencji. Stwierdziliśmy jedynie, że była taka rotacja, nie badaliśmy przyczyn. Odpowiadając na pytanie pana pośła Kazimierza Moskala, czy zdarzyło się wykorzystanie dostępu? – nie, nie zdarzyło się. Niemniej jednak, osoby nie pracujące w danym urzędzie, nadal miały dostęp do systemu. Wdam się w polemikę z panem kierownikiem, dlatego, że nie zmieniono kodu dostępu lub karty i osoba mogła legalnie wchodzić do systemu i korzystać z danych. Nie wiadomo do jakich celów, ale mogła, gdyż miała dostęp. Nasuwa się pytanie, jak często weryfikowana jest lista uprawnionych do dostępu?

Panie pośle Wilczyński, system CEPiK istnieje, badanie prowadziliśmy w zakresie pojazdów i praw jazdy. Obecnie jedynie system CEPiK jest badany pod kątem funkcjonowania i zgodności. Kontrola rozpoczęła się w tym tygodniu. Jeżeli dostęp jest legalny, nie jesteśmy w stanie stwierdzić, czy ktoś używa tych danych do potrzeb służbowych, czy niegodziwych celów.

Dalszą część wypowiedzi przekażę panu dyrektorowi Łubianowi. Bardzo proszę.

Wicedyrektor Departamentu Administracji Publicznej w Najwyższej Izbie Kontroli Dariusz Łubian:

Szanowni państwo, jeżeli chodzi o kwestię zasobów do dyspozycji, stwierdziliśmy, że były szkolenia dla użytkowników w urzędach gmin i urzędach stanu cywilnego. Oczywiście, potrzebne są dalsze działania, ale przede wszystkim edukacja w zakresie bezpieczeństwa. W systemach bezpieczeństwa informacji słabym ogniwem jest człowiek, który robi błędy. Podam przykład z kontroli. W jednym z urzędów miast karty kryptograficzne, służące w pracy do połączenia z aplikacją „Źródło”, znajdowały się w niezamkniętej szufladzie. Wystarczy zatem, że ktoś ma nieodebrane uprawnienia, może legalnie wejść do urzędu. Słabością wykazuje się zawsze człowiek. Zasady bezpieczeństwa powinny być ustalone, wdrożone i przestrzegane. W wielu urzędach nie były w ogóle ustalone, nie było czego egzekwować od pracowników. Wydaje się mi, że to jest podstawowa kwe-

stia. Zawsze pojawia się zagrożenie wycieku danych, zaczyna się od przejęcia uprawnień legalnego użytkownika. To jest podstawowa kwestia. Przede wszystkim trzeba popracować z kierownikami urzędów, żeby poprawić poziom bezpieczeństwa.

Jeżeli chodzi o model integracji, wdrażania dużych projektów, są uznane metodyki zarządzania projektami, ale trzeba je konsekwentnie stosować. Nie można zaczynać jednej metodyki, następnie zmieniać, nie stosować się do zasad w niej przyjętych lub nie przychodzić na spotkania organizowane w trakcie zarządzania projektem. Mam nadzieję, że nie zdarzą się już podobne sytuacje i system będzie sprawnie funkcjonował. Jeżeli pojawią się pytania, jesteśmy do dyspozycji.

Przewodniczący poseł Tadeusz Dziuba (PiS):

Pan poseł Wilczyński, następnie pani przewodnicząca Chrobak. Czy ktoś z państwa posłów chce jeszcze zabrać głos? Bardzo proszę.

Poseł Ryszard Wilczyński (PO):

Zawsze pojawia się problem, gdy zadaje się pytania przekrojowe. Lepiej zadać pytanie szczegółowe, wtedy łatwiej odpowiedzieć. Zadałem konkretne pytanie, czy dostarczono stosowne zasoby do użytkowników końcowych? Powtórzyłem pytanie trzy razy, ale nie doczekałem się odpowiedzi. Pytanie było bardzo konkretne. To pokazuje, jak powinniśmy działać w przyszłości, czy jest nam zawsze potrzebny wojewoda jako pośrednik, wobec plejady od 70 do ponad 300 gmin w województwie. Proszę o odpowiedź na pytanie, czy dostarczono stosowne pod każdym względem – finansowym i ludzkim zasoby, czy wdrożenie przebiegało należycie i zachowano zasady bezpieczeństwa? Wiele zostało powiedziane na temat błędów i zaniechań popełnionych na poziomie gmin.

Na koniec jedna uwaga, proszę spojrzeć na stronę 34. Tam został opisany problem braku funkcji administracji. Jeżeli naprawdę chcemy szkolić użytkowników systemów poprzez filmiki na YouTube, to gratuluje. Może założymy grupę użytkowników na Facebook? A może będą twittować? Tak być nie może. Dziwne, że nie pojawił się wniosek mówiący, iż administracja państwowa musi mieć kanał szkoleniowy. Czy naprawdę państwo uważają, że prawidłowym sposobem szkolenia administracji są filmiki na YouTube? Wydaje się mi, że to jest kwestia do przedyskutowania. Widzę tutaj lukę, która powinna zostać wypełniona. Administracja musi cały czas się doszkalać i wymieniać informacje. Bardzo proszę o odniesienie się do tej kwestii, jak państwo oceniają, czy to jest pożądany model w państwie w XXI w.?

Poseł Barbara Chrobak (Kukiz15):

Panie przewodniczący, odniosę się do słów posła Wilczyńskiego. Rzeczywiście, nie wyobrażam sobie przeprowadzania szkolenia urzędników państwowych na YouTube. To jest dla mnie kuriozum. Chcę jeszcze zapytać odnośnie do dużej ilości pobranych przez komorników danych o numerach PESEL. Są oni uprawnionymi podmiotami, co wynika z przepisów. Natomiast, kto może być nieuprawnionym podmiotem? Jak często jest przeprowadzana kontrola logowania do systemu? Czy są wydruki z takiej kontroli? Nie mamy wiedzy, czy kontrole są w ogóle przeprowadzane. Wiem o czym mówię, gdyż miałam dostęp do numerów PESEL w mojej poprzedniej pracy. Wiem, jak to wygląda – zawsze pozostaje ślad po zarejestrowanej osobie. Czy były przeprowadzane kontrole, które osoby dokonywały logowania i czy miały uprawnienia? Czy nie można rozwiązać problemu w inny sposób, np. poprzez nadanie hasła każdej osobie? Kiedy karta znajduje się w szufladzie i każdy może mieć do niej dostęp, jak powiedział pan prezes NIK. Dziękuję.

Przewodniczący poseł Tadeusz Dziuba (PiS):

Chcę również zadać pytania. Jeśli dobrze zrozumiałem, pytania, które zadał przed chwilą poseł Wilczyński i pani przewodnicząca, są kierowane w dużej mierze do pana ministra, więc czekamy na odpowiedź.

Powiedział pan, że stwierdzono 1000 kategorii błędów w systemie, ale zdarzył się jeden błąd krytyczny. Nie wiem, czy może pan o tym mówić, ale jeśli tak, proszę powiedzieć, dla mojej ciekawości, jakiej kategorii to był błąd? Druga sprawa, pan prezes NIK, w swoim referacie, stwierdził, że administracji rządowej brakuje narzędzi w postaci przepisów. Jeśli państwo podzielają tę opinię, czy jest już projekt nowelizacji odpowied-

niej, nowej ustawy? Jeżeli faktycznie brakuje narzędzi, co w tym zakresie zrobiło Ministerstwo Cyfryzacji? Nie wiem, czy dobrze zrozumiałem, ale pan prezes wymienił termin graniczny – koniec drugiego kwartału 2017 r. (formalnie za trzy tygodnie). Zatem system, o którym mówimy, rejestracji państwowej, powinien być oddany do użytku w pełnym wachlarzu. Czy termin będzie dotrzymany, czy nie?

Ostatnie pytanie. Z odpowiedzi pana dyrektora Centralnego Ośrodka Informatyki wynikało, że system jest całkowicie bezpieczny. W kontekście tego stwierdzenia przypomnę, że według analityków i ekspertów Federacja Rosyjska już prowadzi wojnę, ale nie w realu tylko wirtualną, w przestrzeni cybernetycznej. Niewątpliwie Polska jest na pierwszym froncie. Czy państwo mają pewność, że zasoby informatyczne, będące w dyspozycji administracji rządowej, są zabezpieczone i nie ma do nich żadnego dostępu? Łatwo sobie wyobrazić skutki, jakie mogłyby wywołać, np. zmiany wprowadzone w masowej skali do tych rejestrów. Proszę o odpowiedź. Zaczniemy od pana ministra cyfryzacji.

Podsekretarz stanu w MC Karol Okoński:

Panie przewodniczący, planowałem uzupełnić swoją pierwotną wypowiedź odnośnie do pierwszego pytania posła Wilczyńskiego. Jest ono ważne. Generalnie zgadzam się, że powinniśmy mieć jasno zdefiniowaną metodykę podejścia do realizacji projektu, skutecznie ją powielać, ewentualnie, po każdym projekcie wyciągać wnioski, w jaki sposób uzupełniać, korygować i korzystać z doświadczeń. Dla projektów, które realizuje Ministerstwo Cyfryzacji, mamy przygotowaną metodykę realizacji, bazującą głównie na PRINCE2. Niemniej jednak, jest ona dostosowana do realizacji projektów w administracji publicznej. Jednocześnie zawiera część, którą rekomendujemy, rozpoczynanie wdrożeń etapami tzw. pilotaży, żeby zminimalizować skutki błędów, nie programistycznych, ale dotyczących całego procesu organizacyjno-technicznego danego systemu. Stąd przedsięwzięcie, które realizujemy, np. migracji stanu cywilnego. Jego masowe wdrożenie będzie poprzedzone fazą pilotażu w dwóch miastach. Wybraliśmy je, gdyż zadeklarowały gotowość do uczestnictwa w testach, czyli, jak słusznie pan poseł powiedział, posiadają zasoby, żeby zrealizować zadania, które są im powierzane. Daty wdrożenia poszczególnych *realises* są również konsultowane w ramach grup roboczych, na których są przedstawiciele samorządów, aby odpowiednio uprzedzić i pozwolić im zaplanować prace związane z zadaniami okołowdrożeniowymi. Ich reprezentanci uczestniczą również w testach, jeszcze przed wdrożeniem produkcji.

Jeśli chodzi o kwestię, gdzie plasuje się Ministerstwo Cyfryzacji z perspektywy, np. Systemu Rejestrów Państwowych, dostrzegamy następujący model: mamy różnych właścicieli biznesowych, w tym przypadku Ministerstwo Spraw Wewnętrznych i Administracji, które odpowiada za dane, podstawę prawną, funkcjonalność, łącznie z użytkownikami końcowymi. Ministerstwo Cyfryzacji ma tutaj rolę koordynacyjno-zarządczą, jak również wspiera analizę rozwiązania i przekazuje efekty późniejszych prac, tzw. analizy biznesowej do dostawcy. Realizacja zamawiający – wykonawca znajduje się po stronie Ministerstwa Cyfryzacji, np. COI, ale etap zamawiania poprzedza wcześniejsza, wspólna faza analizy i zbierania wymagań już z właścicielem biznesowym. CEPiK jest dobrym przykładem, gdyż to jest projekt, de facto program, konglomeracja różnych inicjatyw, które powinny być zbieżne w czasie. Stąd, CEPiK został ostatnio przeorganizowany w formę programu z zaproszeniem do komitetu sterującego i międzyresortowego zespołu wszystkich najważniejszych interesariuszy, aby różne inicjatywy, korzystające z bazy centralnej, będące również przedsięwzięciami równoległymi, zgrać w czasie i na bieżąco monitorować ewentualne odstępstwa i problemy, mogące mieć wpływ na poszczególne projekty.

Jeśli chodzi o pytania pana posła odnośnie do szkoleń, filmy na YouTube, przywołane w raporcie, stanowiły uzupełnienie szkoleń. To nie był podstawowy materiał, który miał służyć użytkownikom, jedynie stanowił sposób utrwalenia wiedzy. Zasadnicze szkolenia były prowadzone w formie warsztatów i szkoleń stacjonarnych na tzw. liderów. W szkoleniach wzięło udział ponad 4 tys. urzędników. Ich zadaniem było propagowanie wiedzy w urzędach, w których pracowali. Przy tej okazji powstawała również dokumentacja szkoleniowa. W przypadku projektu CEPiK planowane są warsztaty, ale również

powstanie platforma szkoleniowa, na której będą umieszczane w/w materiały. Odpowiadając na lekkie oburzenie, że wykorzystujemy kanał komercyjny YouTube do szkolenia urzędników, przy tak dużym przedsięwzięciu jak CEPiK, postanowiliśmy przygotować własną platformę, w której będziemy umieszczać materiały szkoleniowe, tym samym ograniczając grono osób mogących mieć dostęp do tej platformy.

Odnośnie do kwestii związanej z bezpieczeństwem, oddam głos panu dyrektorowi Gawrysiowi, żeby odniósł się do kwestii kontrolowania notowań i poziomu uprawnień potrzebnych do korzystania z systemu.

Dyrektor w COI Dariusz Gawryś:

W uzupełnieniu, jeżeli państwo pozwolą, będę próbował powiedzieć precyzyjnie, niemniej jednak, będziemy musieli dotknąć wszystkich obszarów. Nie stwierdziliśmy nieautoryzowanego dostępu. Od strony technicznej wykonaliśmy wszystko, co pozwoliło zabezpieczyć system przed nieautoryzowanym dostępem. Niemniej jednak, jak zauważył pan prezes, pracownik, który ma dostęp, może wykorzystać dane, ale to jest poza zasięgiem rozwiązań technicznych. Nie możemy sobie pozwolić na dalsze kroki związane ze śledzeniem, co dzieje się z tymi danymi. Jeżeli chodzi o logowanie do systemu, powiedziano o karcie, na której jest przechowywany certyfikat, uprawniający do pracy z systemem i wykonywaniem operacji. Oprócz tego, aby zalogować się do systemu potrzebny jest identyfikator i hasło. Ta para stanowi jeden z poziomów zabezpieczeń. Certyfikat włożony do systemu, który nie jest odlogowany, również nie spowoduje, że ktoś będzie miał nieuprawniony dostęp.

Odpowiadając na dwa pytania jednocześnie, odnośnie do bezpieczeństwa w cyberprzestrzeni, powołaliśmy Departament Bezpieczeństwa i w jego ramach mamy zespół techniczny. Państwo słyszeli o określeniu CERT, tj. *Computer Emergency Response Team*, który w przypadku wystąpienia incydentu natychmiast reaguje, podejmując odpowiednie kroki, zarówno techniczne, jak i organizacyjne, jeżeli zostanie wykryty incydent bezpieczeństwa. Zespół również odpowiada za przeglądy, co dzieje się w systemie, czyli jakie były logowania. Oczywiście, nie jesteśmy w stanie przeglądać ich codziennie. Dla zobrazowania sytuacji powiem, że do systemu loguje się ok. 10 tys. użytkowników dziennie i wykonywanych jest ok. 2-3 mln operacji tygodniowo. Wychodząc naprzeciw potrzebom cyberbezpieczeństwa, obecnie jest przygotowany harmonogram i będziemy wdrażać system klasy SIEM, tj. system integracji, informacji o incydentach bezpieczeństwa, który łączy i ma dostęp do różnych systemów oraz obserwuje nienaturalne zachowania. Przykładowo, jeżeli pracownik został zarejestrowany w systemie jako osoba przebywająca na urlopie i nagle loguje się do CEPiK lub SRP, system pokazuje, że operacja jest niemożliwa z punktu widzenia organizacji, a także zespół zostaje natychmiast powiadomiony o incydencie. Taki system mamy zamiar wdrożyć w zintegrowanej sieci rejestrów państwowych, aby odpowiadać na współczesne wyzwania cyberbezpieczeństwa i tego, co nam grozi. Analiza ryzyka pokazuje, że faktycznie, ingerencja w dane oraz ich nieautoryzowany wyciek spowodowałyby naprawdę duże konsekwencje. Z najwyższą starannością podchodzimy do zagadnień bezpieczeństwa.

Odpowiadając na pytanie odnośnie do incydentu krytycznego, system jest rozwijany, co pół roku wydajemy nową wersję, zawierającą zmiany związane z nowościami technicznymi, rozwojowymi i uwagami odnoszącymi się do funkcjonalności. Przed wdrożeniem nowa wersja systemu jest testowana z grupami użytkowników, przez specjalne systemy, które sprawdzają poszczególne funkcjonalności. Niemniej jednak, przy oddawaniu takiego systemu zdarzają się czasami błędy. Dokładnie taki błąd nastąpił w bazie usług stanu cywilnego. Okazało się, że w trakcie pobierania danych do wyświetlenia projektów aktów, zapytanie z aplikacji „Źródło” do bazy danych nie było optymalne i powodowało tak duże obciążenie serwerów, iż inni użytkownicy nie mogli pracować (jest to jedna z funkcji dla urzędnika stanu cywilnego), w związku z tym system został wstrzymany na godzinę. W tym czasie poprawiliśmy zapytanie i po 45 min. od poprawki i przetestowania rozwiązania, zostało ono wgrane na produkcję. W sumie system był w niewielkim stopniu dostępny przez dwie godziny. Niektóre operacje mogły być prowadzone, np. w rejestrze PESEL lub dowodów osobistych.

Podsekretarz stanu w MC Karol Okoński:

Chcę jeszcze uzupełnić. Pojawiło się pytanie o dwie kwestie. Pierwsza dotyczyła migracji stanu cywilnego, czy utrzymamy termin drugiego kwartału bieżącego roku, czyli faktycznie za kilka tygodni? Jesteśmy na ostatnim etapie testów i obecnie planowana data wdrożenia to 23 czerwca. Istnieje ryzyko, że data może ulec przesunięciu o tydzień lub dwa z racji dodatkowych prac związanych z komponentem niejawnym. Jednak, chcemy dotrzymać wcześniej deklarowanego terminu drugiego kwartału. Jeśli pojawi się przesunięcie to zaledwie o kilka dni. Odnośnie do przepisów, których brakuje, żeby wyegzekwować od użytkowników niektóre sprawy dotyczące bezpieczeństwa, jesteśmy na etapie opracowywania całościowej polityki bezpieczeństwa i po jej przygotowaniu będziemy równolegle zastanawiali się, jakie kwestie można przekładać na konkretne przepisy. Aktualnie jeszcze nie mamy projektu zmian przepisów.

Wiceprezes NIK Mieczysław Łuczak:

Panie przewodniczący, odpowiadając na pytania pana posła Wilczyńskiego, bardzo chciałbym, żeby w Polsce była instytucja, która sprawdza, daje zalecenia i nadzoruje wykonanie. Takiej kompetencji nie posiadamy, w związku z tym, nie jesteśmy w stanie zrealizować tego pomysłu. Gwoli uzupełnienia wypowiedzi pana ministra, od 10 do 12 grudnia 2014 r. oraz od 19 do 23 stycznia 2015 r. egzamin z modułu PESEL zdało w sumie 7 100 użytkowników, z modułu RDO 6 745 osób i z modułu BUSK 5 482 osoby. Do egzaminu przystąpiło łącznie 19 327 osób, zdało 10 025. Zatem, egzaminy i szkolenia były przeprowadzane, a filmiki na YouTube stanowiły uzupełnienie. Natomiast, odpowiadając panu przewodniczącemu, jaki był zakres, co stwierdziliśmy i czego brakowało w ochronie bezpieczeństwa? Na bazie wyników kontroli, 62% zbadanych nie opracowało i nie wdrożyło polityki bezpieczeństwa informacji wymaganej przez przepisy prawa, 23% nie przestrzegało wymogów zablokowania dostępu do Internetu na komputerach wykorzystywanych w systemie, w 38% badanych przypadków wystąpiły nieprawidłowości w zakresie blokowania i odebrania dostępu. O tym była dyskusja. Podobnych przypadków jest więcej. W szczególności, w polityce bezpieczeństwa projektów brakuje: zdefiniowanych procedur komunikacji między COI, a ministerstwem pełniącym funkcję zarządcy w zakresie systemu; zarządzania kontami użytkowników; nadawania i administrowania uprawnień; pełnej, zdefiniowanej polityki zarządzania kontrolą dostępu do systemu polityki bezpieczeństwa osobowego oraz systemu zarządzania ciągłością działania. 61% Polaków chce korzystać z takich systemów i udogodnień. Kierunek jest dobry, ale trzeba go realizować precyzyjniej. Odnośnie do terminu, panie przewodniczący, pani minister Streżyńska, w piśmie do pani prezes Polkowskiej, zadeklarowała, że 12 maja minie termin pierwszego etapu.

Przewodniczący poseł Tadeusz Dziuba (PiS):

Dziękuję za odpowiedź...

Poseł Ryszard Wilczyński (PO):

Chcę powiedzieć jedno zdanie. Niech YouTube pozostanie jako inspiracja. Pan minister powiedział bardzo celnie – potrzebujemy platformy e-learningowej dla administracji publicznej.

Głos z sali:

Ale to było powiedziane, panie pośle, tu jest napisane.

Poseł Ryszard Wilczyński (PO):

Czyli jest już platforma e-learningowa i możemy się szkolić, tak? OK, jeżeli istnieje, to dobrze.

Przewodniczący poseł Tadeusz Dziuba (PiS):

Dziękuję za obfitą dyskusję. Dziękuję naszym gościom za udzielenie odpowiedzi. Rozumiem, że możemy przyjąć do wiadomości informację Najwyższej Izby Kontroli, dodając, że administracja publiczna nie najlepiej radzi sobie z zarządzaniem i zapewnianiem bezpieczeństwa państwowym systemom informatycznym. Mam nadzieję, że w tym zakresie, jak państwo sygnalizowali w swoich wypowiedziach, będzie istotny postęp.

Przechodzimy do drugiego punktu – sprawy bieżące. Pozwolą państwo, że w ramach spraw bieżących powiem o trzech kwestiach. Po pierwsze, przewodniczący sejmowej Komisji Ochrony Środowiska, Zasobów Naturalnych i Leśnictwa skierował pismo do pana przewodniczącego sejmowej Komisji do Spraw Kontroli Państwowej. Przeczytam je: „Zgodnie z wnioskiem pani poseł Agaty Borowiec zgłoszonym na posiedzeniu sejmowej Komisji Ochrony Środowiska, Zasobów Naturalnych i Leśnictwa o doprecyzowanie tematu kontroli, zaproponowanego przez Komisję do planu pracy Najwyższej Izby Kontroli, pragnę poinformować, że Komisja przegłosowała zmianę brzmienia tematu. W związku z powyższym, uprzejmie proszę o wycofanie tematu: «Kontrola działań prowadzonych i zleczanych przez Ministerstwo Środowiska i podmioty nadzorowane w Puszczy Białowieskiej» nr 54 i zastąpienie go tematem: «Stan formalno-prawny Puszczy Białowieskiej od momentu ustanowienia sieci obszarów Natura 2000, ze szczególnym uwzględnieniem strat powstałych po 2008 r.»”. Wydaje się mi, że drugie sformułowanie jest precyzyjniejsze, zwłaszcza z punktu widzenia NIK. Jeśli nie usłyszę sprzeciwu uznaję, że Komisja wyraża zgodę, aby pod pozycją nr 54 w naszym wykazie znalazł się zbliżony temat, ale w nowym ujęciu. Dziękuję.

Druga sprawa. Państwo już wiedzą, ale muszę powiedzieć, że jutro o godz. 10.00 odbędzie się kolejne posiedzenie naszej Komisji z udziałem pana Janusza Wojciechowskiego, członka Europejskiego Trybunału Obrachunkowego, byłego prezesa Najwyższej Izby Kontroli, który złożył nam informację na temat rocznego sprawozdania z działalności Trybunału.

Kolejna sprawa, pojawiła się prośba, aby do planu pracy Komisji na okres drugiego półrocza, czyli od 1 lipca do 31 grudnia, złożyć propozycje tematów posiedzeń naszej Komisji. Pan przewodniczący wyznaczył termin graniczny 19 czerwca. Zatem, proszę państwa, żeby w ciągu 10 dni przedstawić własne propozycje tematów pracy Najwyższej Izby Kontroli. Ostatni komunikat, po obecnych obradach odbędzie się posiedzenie Prezydium Komisji. Czy ktoś z pań i panów posłów chce wnieść jakąkolwiek sprawę? Nie słyszę. Dziękuję. Kończymy posiedzenie Komisji.