



**WICEPREZES
NAJWYŻSZEJ IZBY KONTROLI**
Wojciech Kutyla

KPB – 4101-002-01/2014

P/14/043

**WYSTĄPIENIE
POKONTROLNE**

I. Dane identyfikacyjne kontroli

Numer i tytuł kontroli P/14/043 - Realizacja przez podmioty państwowe zadań w zakresie ochrony cyberprzestrzeni Rzeczypospolitej Polskiej

Jednostka przeprowadzająca kontrolę Najwyższa Izba Kontroli
Departament Porządku i Bezpieczeństwa Wewnętrznego

Kontroler Paweł Gibuła, doradca ekonomiczny, upoważnienie do kontroli nr 89665 z dnia 2 czerwca 2014 r.

(dowód: akta kontroli tom I str. 1-2)

Jednostka kontrolowana Ministerstwo Administracji i Cyfryzacji (zwane dalej MAiC), ul. Królewska 27, 00-060 Warszawa

Kierownik jednostki kontrolowanej Andrzej Halicki, Minister Administracji i Cyfryzacji – od dnia 22 września 2014 r.
Poprzednio, w okresie objętym kontrolą, funkcję Ministra Administracji i Cyfryzacji sprawowali:

- Pan Rafał Trzaskowski – od 3 grudnia 2013 r. do 22 września 2014 r.;
- Pan Michał Boni – od 18 listopada 2011 r. do 27 listopada 2013 r.

Kontrolą objęto okres od daty utworzenia Ministerstwa Administracji i Cyfryzacji (18 listopada 2011 r.) do dnia zakończenia czynności kontrolnych (5 grudnia 2014 r.)

(dowód: akta kontroli tom I str. 3)

II. Ocena kontrolowanej działalności

Ocena ogólna

W ocenie NIK¹, w całym okresie objętym kontrolą, w MAiC nie zidentyfikowano w sposób rzetelny i kompleksowy, jakie zadania powinny być realizowane przez Ministra Administracji i Cyfryzacji w związku z ochroną cyberprzestrzeni RP. Nie przypisano również zasobów oraz nie zbudowano potencjału kadrowego i merytorycznego adekwatnego do wykonywania tych zadań. W rezultacie, Minister Administracji i Cyfryzacji praktycznie nie realizował zadań związanych z inicjowaniem i koordynacją działań w zakresie bezpieczeństwa teleinformatycznego państwa oraz w ogóle nie realizował zadań związanych z koordynacją krajowego systemu reagowania na incydenty komputerowe w cyberprzestrzeni RP. Ograniczone działania zostały rozpoczęte w zasadzie dopiero od stycznia 2014 roku, jednak ze względu na brak wystarczających zasobów kadrowych oraz nierzetelne przygotowanie działań, zadania Ministra były realizowane fragmentarycznie lub z dużym opóźnieniem.

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

III. Opis ustalonego stanu faktycznego

1. Budowa systemu ochrony cyberprzestrzeni RP.

1.1. Opracowanie narodowej strategii ochrony cyberprzestrzeni.

Opis stanu
faktycznego

W styczniu 2012 r., na podstawie decyzji Zespołu zadaniowego do spraw ochrony portali rządowych², w MAiC wznowiono prace prowadzone wcześniej w byłym Ministerstwie Spraw Wewnętrznych i Administracji³, mające na celu przygotowanie strategicznego dokumentu dotyczącego bezpieczeństwa teleinformatycznego państwa. Prace nad tym dokumentem były prowadzone przez Członków Zespołu zadaniowego do spraw ochrony portali rządowych oraz przez pracowników Gabinetu Politycznego Ministra Administracji i Cyfryzacji. W wyniku ww. prac, przygotowano projekt dokumentu pt. *Polityka Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej* (zwany dalej *Polityką*), który we wrześniu 2012 r. został przekazany przez Ministra Administracji i Cyfryzacji do konsultacji międzyresortowych i społecznych, a następnie w marcu 2013 r., do rozpatrzenia przez Stały Komitet Rady Ministrów.

Była Szefowa Gabinetu Politycznego Ministra Administracji i Cyfryzacji - Pani Marlena Niewiadomska zeznała, iż decyzja o przyjęciu krajowej strategii ochrony cyberprzestrzeni w formie polityki, w miejsce pierwotnie planowanego programu rządowego, została podjęta przez Zespół zadaniowy do spraw ochrony portali rządowych. Wskazała również, iż było to spowodowane wymogami ustawy o zasadach polityki rozwoju, dotyczącymi zawartości programów rządowych oraz dążeniem do jak najszybszego przyjęcia dokumentu wprowadzającego przynajmniej minimalne obowiązki związane z podniesieniem bezpieczeństwa systemów teleinformatycznych administracji rządowej.

(dowód: akta kontroli tom I str. 375-382, tom II str. 1-369)

Uwagi zgłaszane przez podmioty państwowe do projektu *Polityki* dotyczyły m.in.: doprecyzowania terminologii używanej w tym dokumencie, przeredagowania pkt 1.5., w którym wskazano instytucje odpowiadające za bezpieczeństwo cyberprzestrzeni RP oraz podkreślenia, że *Polityka* nie będzie implikować dodatkowych środków finansowych z budżetu państwa w roku jej wejścia w życie (uwaga Ministerstwa Finansów).

MAiC otrzymało również liczne uwagi instytucji pozarządowych⁴ wskazujące na braki merytoryczne *Polityki* dotyczące w szczególności:

- nieprawidłowego zakresu podmiotowego tego dokumentu, tj. ograniczenia jego obowiązywania do administracji rządowej oraz braku adekwatnego odniesienia do podmiotów prywatnych, w tym zarządzających teleinformatyczną infrastrukturą krytyczną państwa;

² Zespół zadaniowy do spraw ochrony portali rządowych został powołany decyzją Przewodniczącego Komitetu Rady Ministrów do spraw Cyfryzacji Nr 1/2012 z dnia 24 stycznia 2012 r., w reakcji na ataki przeprowadzone w styczniu 2012 r. na najważniejsze strony internetowe administracji publicznej (tzw. protesty ACTA). Celami działania Zespołu było w szczególności wypracowanie wytycznych ochrony portali rządowych oraz ustalenie standardów bezpieczeństwa dla stron rządowych. W skład Zespołu wchodził przedstawiciel: Agencji Bezpieczeństwa Wewnętrznego, Ministra Obrony Narodowej, Ministra Spraw Wewnętrznych, Ministra Sprawiedliwości, Ministra Spraw Zagranicznych, Szefa Kancelarii Prezesa Rady Ministrów oraz Rządowego Centrum Legislacji. Przewodniczącym Zespołu był Minister Administracji i Cyfryzacji, a podległe mu Ministerstwo zapewniało obsługę administracyjno-biurową Zespołu. Ww. Zespół został formalnie rozwiązany w dniu 13 czerwca 2014 r.

³ W latach 2008-2011 w byłym Ministerstwie Spraw Wewnętrznych i Administracji (MSWiA) oraz m.in. w Agencji Bezpieczeństwa Wewnętrznego (ABW) opracowano 7 kolejnych projektów narodowej strategii bezpieczeństwa cyberprzestrzeni. Żaden z tych projektów nie został zatwierdzony przez Radę Ministrów i przyjęty formalnie do realizacji.

⁴ Podmiotami, które przekazały do MAiC uwagi dot. treści projektu *Polityki* były m.in.: Polskie Towarzystwo Informatyczne, Polska Konfederacja Pracodawców Prywatnych Lewiatan, Instytut Kościuszki, Polska Izba Informatyki i Telekomunikacji, Stowarzyszenie Euro-Atlantyckie, Fundacja Bezpieczna Cyberprzestrzeń, Fundacja Instytut Mikromakro.

- nieprecyzyjnego brzmienia zapisów *Polityki* – nieokreślenia zadań, terminów ich realizacji, mierników oraz podmiotów odpowiedzialnych za ich wykonanie;
- braku oszacowania kosztów i niewskazania źródeł finansowania działań wskazanych w *Polityce*.

Polityka Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej została przyjęta uchwałą Rady Ministrów z dnia 25 czerwca 2013 r.⁵, a koordynację jej realizacji powierzono ministrowi właściwemu ds. informatyzacji. Zgodnie z pkt 1.4. *Polityki*:

- obowiązuje ona podmioty administracji rządowej;
- jest rekomendowana dla jednostek samorządu terytorialnego oraz innych podmiotów i instytucji państwowych;
- stanowi wskazówkę dla wszystkich innych użytkowników cyberprzestrzeni.

(dowód: akta kontroli tom II str. 1-370)

Z udzielonych wyjaśnień wynika, iż ograniczenie obowiązywania *Polityki* do podmiotów administracji rządowej oraz zmiana zakresu oddziaływania tego dokumentu w stosunku do propozycji zawartych w opracowanych wcześniej w MSWiA projektach programów rządowych dotyczących ochrony cyberprzestrzeni, wynikały z uwag Rządowego Centrum Legislacji wskazujących, iż *Polityka* nie może obowiązywać podmiotów spoza administracji rządowej.

Pan Roman Dmowski - Podsekretarz Stanu w MAiC odpowiadający za realizację zadań związanych z ochroną cyberprzestrzeni zeznał, iż w jego ocenie zakres podmiotowy *Polityki* został określony w sposób prawidłowy i nie jest uzasadnione, aby ten dokument odnosił się w pierwszej kolejności do (państwowych i prywatnych) operatorów infrastruktury krytycznej. Wskazał, że ustawa o zarządzaniu kryzysowym już reguluje obszary infrastruktury krytycznej, natomiast przed przyjęciem *Polityki* brakowało dokumentu adresującego działania uświadamiające i podnoszące bezpieczeństwo IT na poziomie poszczególnych urzędów.

(dowód: akta kontroli tom I str. 4-40, 120-123, tom III str. 464-474)

Od momentu zatwierdzenia *Polityki*, w MAiC nie były dokonywane przeglądy treści tego dokumentu oraz nie prowadzono prac mających na celu jego aktualizację. Z udzielonych wyjaśnień wynika, że nie podejmowano takich działań, ponieważ wprowadzenie zmian do *Polityki* byłoby przedwczesne z uwagi na trwające prace nad dyrektywą o zapewnieniu wspólnego, wysokiego poziomu bezpieczeństwa sieci i informacji (zwaną dalej dyrektywą NIS). Podsekretarz Stanu w MAiC wyjaśnił, że: *Ewentualne zmiany „Polityki ochrony cyberprzestrzeni RP” muszą być spójne z zapisami dyrektywy, które jednak mogą nadal ulec zmianie. (...) jest jednak niemal pewne, że ostatecznie przyjęte przepisy wymuszą stworzenie nowego dokumentu strategicznego w tym zakresie. W takiej sytuacji podejmowanie prób uaktualnienia Polityki wydaje się bezcelowe (...).*

(dowód: akta kontroli I str. 4-40)

Ustalone
nieprawidłowości

Kontrola wykazała, że działania Ministra Administracji i Cyfryzacji mające na celu opracowanie narodowej strategii ochrony cyberprzestrzeni były prowadzone w sposób nierzetelny i bez właściwego przygotowania. Na etapie prac nad projektem *Polityki*, nie przeprowadzono kluczowych analiz pozwalających na zapewnienie wysokiej jakości merytorycznej tego dokumentu. Nie wykorzystywano dostępnych w tym zakresie wzorów dobrych praktyk⁶ oraz uwag instytucji pozarządowych zgłoszonych na etapie konsultacji społecznych projektu *Polityki*, i tak:

⁵ Nr 111/2013.

⁶ Zob. np.: European Network and Information Security Agency, National Cyber Security Strategies, Practical Guide on Development and Execution, grudzień 2012 r.

- na etapie wyodrębnienia MAiC z byłego MSWiA, nie dokonano przejęcia materiałów i dokumentacji wytworzonych w ramach prowadzonych w tej instytucji w latach 2008-2011 prac, związanych z ochroną cyberprzestrzeni RP i przyjęciem narodowej strategii ochrony cyberprzestrzeni;
- nie została przeprowadzona kompleksowa inwentaryzacja obowiązujących aktów prawnych związanych z ochroną cyberprzestrzeni RP;
- nie opracowano katalogu kluczowych dla funkcjonowania państwa systemów teleinformatycznych, które powinny podlegać ochronie. W szczególności: nie prowadzono współpracy z Rządowym Centrum Bezpieczeństwa (RCB) w zakresie określenia kryteriów identyfikacji oraz ewentualnego wykorzystania opracowanego przez ten podmiot wykazu infrastruktury krytycznej (w zakresie ujętych w tym wykazie systemów teleinformatycznych) oraz nie pozyskano, ani nie opracowano wykazu systemów teleinformatycznych wykorzystywanych do realizacji zadań publicznych⁷;
- nie oszacowano zasobów i kosztów niezbędnych do realizacji działań wskazanych w *Polityce*.

Była Szefowa Gabinetu Politycznego Ministra Administracji i Cyfryzacji zeznała, że nie przeprowadzono tego rodzaju analiz na etapie prac nad *Polityką*, ponieważ nie otrzymała takiego polecenia od przełożonych. Wskazała również, że decyzje dotyczące treści *Polityki* były podejmowane przez Członków Zespołu zadaniowego do spraw ochrony portali rządowych.

Podsekretarz Stanu w MAiC – Pan Roman Dmowski wyjaśnił, iż: *Należy podkreślić, że „Polityka ochrony cyberprzestrzeni RP” została opracowana w ramach prac Zespołu zadaniowego do spraw ochrony portali rządowych (...), a nie w ramach prac ministerstwa.*

(dowód: akta kontroli tom I str. 4-68, 120-123, 375-382, 383-387, 464-474, tom II str. 1-370, tom V str. 1-119)

W ocenie NIK, nie można uznać za zasadne wyjaśnień Kierownictwa MAiC wskazujących, że podmiotem odpowiedzialnym za przygotowanie *Polityki* był Zespół zadaniowy do spraw ochrony portali rządowych. Zdaniem NIK, organem odpowiedzialnym za opracowanie narodowej strategii ochrony cyberprzestrzeni był Minister Administracji i Cyfryzacji⁸, kierujący działami administracji rządowej informatyzacja i łączność⁹, podczas gdy ww. Zespół stanowił tylko ciało pomocnicze Komitetu Rady Ministrów do spraw Cyfryzacji. Powierzenie zadań związanych z opracowaniem narodowej strategii ochrony cyberprzestrzeni Zespołowi zadaniowemu do spraw ochrony portali rządowych oraz Gabinetowi Politycznemu Ministra świadczą natomiast o tym, że w MAiC nie został wdrożony system realizacji zadań związanych z ochroną cyberprzestrzeni. Nie przypisano zasobów do ich wykonywania oraz nie zdefiniowano w sposób kompleksowy, jakie zadania powinny być w tym zakresie realizowane przez Ministra Administracji i Cyfryzacji (kwestie te szczegółowo opisano w pkt III.1.1.2. wystąpienia pokontrolnego). Należy również podkreślić, że ww. Zespół zadaniowy powstał w reakcji na konkretne wydarzenia społeczne¹⁰ i realizował precyzyjnie wskazane zadania dotyczące bezpieczeństwa

⁷ W rozumieniu ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2014 r., poz. 1114.).

⁸ Wcześniej – Minister Spraw Wewnętrznych i Administracji.

⁹ Na podstawie § 1 ust. 2 pkt 2-3 rozporządzenia Prezesa Rady Ministrów z dnia 22 września 2014 r. w sprawie szczegółowego zakresu działania Ministra Administracji i Cyfryzacji (Dz. U. z 2014 r., poz. 1254.). Poprzednio, w okresie objętym kontrolą, rozporządzenie Prezesa Rady Ministrów z dnia 18 listopada 2011 r. w sprawie szczegółowego zakresu działania Ministra Administracji i Cyfryzacji (Dz. U. Nr 248, poz. 1479.).

¹⁰ Tzw. protesty ACTA, które skutkowały atakami na najważniejsze strony internetowej administracji publicznej.

portali rządowych. Przygotowanie *Polityki* przez Zespół wpłynęło zatem negatywnie na jakość tego dokumentu, m.in. poprzez zdeterminowanie jego zakresu podmiotowego i ograniczenie jego obowiązywania do podmiotów administracji rządowej.

Osobą odpowiedzialną za powstanie opisanych powyżej nieprawidłowości jest były Minister Administracji i Cyfryzacji – Pan Michał Bonii. Do dnia podpisania niniejszego wystąpienia pokontrolnego, Pan Michał Bonii nie złożył wyjaśnień w ww. kwestiach.

(dowód: akta kontroli tom III str. 477-480)

Uwagi dotyczące
badanej działalności

NIK zwraca uwagę, że *Polityka Ochrony Cyberprzestrzeni RP* jest dokumentem nieprecyzyjnym i wzbudzającym liczne wątpliwości interpretacyjne. W *Polityce* nie określono: celów, produktów, mierników, terminów realizacji poszczególnych zadań, podmiotów odpowiedzialnych za ich wykonanie, ani zasobów (w szczególności finansowych) niezbędnych do ich realizacji. W ww. dokumencie nie wskazano również żadnych propozycji zmian legislacyjnych koniecznych do wprowadzenia w celu wdrożenia systemu ochrony cyberprzestrzeni RP. Zapisy *Polityki* zostały sformułowane w sposób nienormatywny i niejednoznaczny (z użyciem trybu przypuszczającego), w związku z czym nie określają one jednoznacznych i precyzyjnych zobowiązań podmiotów państwowych. Należy również podkreślić, że wątpliwości interpretacyjne dotyczące treści *Polityki* były wielokrotnie zgłaszane w toku kontroli przez pracowników i Członka Kierownictwa MAiC odpowiadających za wdrażanie tego dokumentu. Powyższe, zdaniem NIK, świadczy o niskiej jakości *Polityki* oraz o ograniczonych możliwościach jej praktycznego zastosowania w celu podniesienia poziomu bezpieczeństwa teleinformatycznego państwa.

1.2. Przypisanie zasobów do realizacji zadań związanych z ochroną cyberprzestrzeni RP.

Opis stanu
faktycznego

W okresie od utworzenia MAiC w listopadzie 2011 r., do grudnia 2013 r., zadania związane z ochroną cyberprzestrzeni były realizowane przez Gabinet Polityczny Ministra Administracji i Cyfryzacji, w tym, przez większość tego okresu przez jedną osobę – Szefową Gabinetu Politycznego¹¹. Dopiero od stycznia 2014 r. zadania związane z ochroną cyberprzestrzeni przypisano (początkowo nieformalnie – na podstawie polecenia wydanego przez Podsekretarza Stanu w MAiC, a formalnie od sierpnia 2014 r. na podstawie zmienionego regulaminu organizacyjnego Ministerstwa) komórce merytorycznej Ministerstwa, tj. Wydziałowi Unii Europejskiej i Spraw Międzynarodowych Departamentu Społeczeństwa Informacyjnego (DSI). Początkowo, w ramach ww. komórki organizacyjnej, przedmiotowe zadania były realizowane przez dwóch pracowników - absolwentów kierunków humanistycznych, nie mających wykształcenia i doświadczenia zawodowego bezpośrednio związanych z bezpieczeństwem informacji i bezpieczeństwem teleinformatycznym. W sierpniu i listopadzie 2014 r., Wydział Unii Europejskiej i Spraw Międzynarodowych został wzmocniony 2 nowymi pracownikami. Pierwsza z zatrudnionych osób miała wykształcenie humanistyczne i nie posiadała dotychczas (poza stażami) żadnego doświadczenia zawodowego, natomiast rozpoczęła samodzielnie doksztalcenie w zakresie tematyki związanej m.in. z bezpieczeństwem informacji. Drugi z nowo zatrudnionych pracowników posiadał doświadczenie i wykształcenie w zakresie bezpieczeństwa informacji.

¹¹ Od marca 2013 r. w realizacji zadań związanych z ochroną cyberprzestrzeni uczestniczył drugi pracownik Gabinetu Politycznego, a w okresie lipiec – wrzesień 2013 r. dodatkowy pracownik biorący udział w opracowaniu założeń audytu wewnętrznego w obszarze bezpieczeństwa IT instytucji publicznych. Pracownicy z innych komórek organizacyjnych Ministerstwa (Departament Prawny, Departament Telekomunikacji, Departament Informatyzacji) zgodnie z udzielonymi wyjaśnieniami, uczestniczyli w pojedynczych zadaniach związanych tematycznie z ochroną cyberprzestrzeni, np. w przygotowaniu stanowiska do dyrektywy NIS.

Od dnia 18 września 2013 r., zadania związane z ochroną cyberprzestrzeni zostały przypisane do zakresu czynności Podsekretarza Stanu w MAiC – Pana Romana Dmowskiego¹².

(dowód: akta kontroli tom I str. 4-40, 69-75, 124-152, 376-382, tom III str. 391-419)

Odnośnie działań podejmowanych obecnie w celu rozbudowy potencjału kadrowego do realizacji zadań związanych z ochroną cyberprzestrzeni, Podsekretarz Stanu w MAiC – Pan Roman Dmowski zeznał, że: *Realizacja wszystkich celów opisanych w Polityce wymaga znacznie większych niż w chwili obecnej zasobów kadrowych i zatrudnienia najwyższej klasy specjalistów z zakresu cyberbezpieczeństwa. W chwili obecnej jesteśmy na etapie opracowywania krótkoterminowego planu działania dla komórki organizacyjnej MAiC zajmującej się kwestiami cyberbezpieczeństwa, który ma określić zadania na najbliższe 2 lata. W dokumencie tym zostaną doprecyzowane zadania wynikające z Polityki oraz zostanie zapewniona jego kompatybilność z Planem działań opracowywanym przez Zespół międzyresortowy. Zdefiniowanie zbioru zadań pozwoli określić obszary, w których należy wzmocnić skład osobowy zespołu. Jest to na razie wstępny projekt tego dokumentu, którego pierwsza wersja powstanie być może do końca roku. Z mojej wiedzy wynika, że na chwilę obecną nie są prowadzone postępowania kadrowe, mające na celu znaczące rozbudowanie składu osobowego tego Zespołu.*

(dowód: akta kontroli tom III str. 466-474)

W latach 2012-2014¹³, wydatki MAiC na realizację zadań związanych z ochroną cyberprzestrzeni RP wyniosły łącznie 771,3 tys. zł (w tym 760,2 tys. zł z budżetu państwa oraz 11,1 tys. zł ze środków UE) i dotyczyły one:

- współpracy międzynarodowej i wyjazdów służbowych pracowników Ministerstwa - 64,9 tys. zł;
- kampanii społecznych o charakterze edukacyjno-prewencyjnym dotyczących korzystania z Internetu i bezpieczeństwa w cyberprzestrzeni – 688,0 tys. zł¹⁴;
- zakupu metodyki szacowania ryzyka - 3,7 tys. zł;
- szkoleń i konferencji organizowanych przez MAiC, dotyczących bezpieczeństwa teleinformatycznego – 14,7 tys. zł (z tego 11,1 tys. zł ze środków UE).

(dowód: akta kontroli tom I str. 270-281)

Na etapie prac nad przygotowaniem projektu budżetu na 2014 r. oraz Wieloletniego Planu Finansowego Państwa 2013-2016, Minister Administracji i Cyfryzacji zgłaszał potrzeby dotyczące zabezpieczenia środków finansowych na budowę autonomicznego systemu wykrywania, identyfikacji oraz analizy ataków i zagrożeń w cyberprzestrzeni. Zgłoszone zapotrzebowanie nie zostało uwzględnione z powodu konieczności ograniczania wydatków budżetu państwa. Prowadzono również konsultacje z Ministerstwem Finansów (MF) dotyczące stanowiska Polski odnośnie oczekiwanych skutków finansowych dyrektywy NIS, w toku których MAiC podnosiło m.in., iż nie jest możliwe wypracowanie rozwiązań nie powodujących dodatkowego obciążenia dla budżetu. Stanowisko MF wskazywało natomiast na brak akceptacji jakichkolwiek rozwiązań generujących dodatkowe wydatki.

¹² Decyzja Nr 9 Ministra Administracji i Cyfryzacji z dnia 11 czerwca 2013 r. w sprawie zakresu czynności Sekretarza Stanu, Podsekretarza Stanu oraz Dyrektora Generalnego Ministerstwa Administracji i Cyfryzacji (Dz. Urz. MAiC z 2013 r., poz. 16 ze zm.).

¹³ Wg stanu na dzień 30 września 2014 r.

¹⁴ Z tego, wydatki w wysokości 686,5 tys. zł poniesiono na podstawie 4 umów dotacji zawartych w wyniku konkursów ofert przeprowadzonych na podstawie ustawy z dnia 24 kwietnia 2003 r. o działalności pożytku publicznego i o wolontariacie (Dz. U. z 2014 r., poz. 1118 ze zm.).

Poza dwoma ww. przypadkami, Minister Administracji i Cyfryzacji nie występował do Ministra Finansów o przeznaczenie dodatkowych środków na realizację zadań związanych z ochroną cyberprzestrzeni. Jak wyjaśnił Minister Administracji i Cyfryzacji uznano, że dyskusja prowadzona z MF na temat skutków finansowych dyrektywy NIS w wystarczający sposób odzwierciedla problemy związane z wykonywaniem zadań dotyczących ochrony cyberprzestrzeni.

(dowód: akta kontroli tom III str. 410-463)

Minister Administracji i Cyfryzacji nie informował Prezesa Rady Ministrów o ograniczeniach kadrowych i finansowych uniemożliwiających rzetelną realizację zadań związanych z ochroną cyberprzestrzeni, w tym dotyczących koordynacji wdrażania *Polityki* oraz krajowego systemu reagowania na incydenty komputerowe w cyberprzestrzeni RP.

Podsekretarz Stanu w MAiC – Pan Roman Dmowski zeznał: *Od lat obowiązuje reguła dot. zamrożenia wynagrodzeń w administracji publicznej. Ponieważ Rada Ministrów precyzyjnie wskazała w Polityce, że wdrażanie tego dokumentu nie będzie implikować dodatkowych środków finansowych, nie zwracaliśmy się do Prezesa Rady Ministrów o ponowne wyjaśnienie tej kwestii.*

(dowód: akta kontroli tom III str. 466-476)

Zasoby do realizacji zadań związanych z ochroną sieci i systemów teleinformatycznych wykorzystywanych przez MAiC.

W przypadku 5 systemów teleinformatycznych przeznaczonych do realizacji zadań Ministra Administracji i Cyfryzacji, obowiązki związane z utrzymaniem i zapewnieniem bezpieczeństwa tych systemów zostały przekazane do Centrum Projektów Informatycznych¹⁵.

Zgodnie z § 28 ust. 1 pkt 14 regulaminu organizacyjnego Ministerstwa Administracji i Cyfryzacji¹⁶, sprawowanie nadzoru nad bezpieczeństwem wewnętrznych sieci i systemów teleinformatycznych Ministerstwa należało do obowiązków Biura Dyrektora Generalnego (BDG). Wg stanu na dzień 20 listopada 2014 r., zadania w ww. zakresie były realizowane przez 5 pracowników Wydziału Informatyki BDG.

Ponadto, w trakcie kontroli NIK, w dniu 14 sierpnia 2014 r., w MAiC powołany został *Pełnomocnik do spraw bezpieczeństwa cyberprzestrzeni*, któremu powierzono prowadzenie spraw związanych z bezpieczeństwem krytycznych systemów teleinformatycznych wykorzystywanych do realizacji zadań publicznych przez Ministra Administracji i Cyfryzacji oraz systemu teleinformatycznego Ministerstwa.

(dowód: akta kontroli tom I str. 383-475)

W MAiC nie została wydzielona odrębna komórka organizacyjna odpowiadająca za bezpieczeństwo jawnych systemów teleinformatycznych, a zadania z zakresu bezpieczeństwa były wykonywane przez te same osoby, które administrują systemami Ministerstwa.

Minister Administracji i Cyfryzacji wyjaśnił, że z uwagi na ograniczone zasoby kadrowe wystąpiła konieczność kumulacji zadań w Wydziale Informatyki BDG. Poinformował, że docelowo planowane jest powołanie w MAiC wewnętrznego zespołu reagowania na incydenty komputerowe.

(dowód: akta kontroli tom I str. 383-475)

¹⁵ System elektronicznej Platformy Usług Administracji Publicznej, system Publikatora Aktów Prawnych, Scentralizowany System Dostępu do Informacji Publicznej, Strona Główna Biuletynu Informacji Publicznej oraz budowany system obsługi zbiorów publicznych.

¹⁶ Stanowiącego załącznik do Zarządzenia Nr 3 Ministra Administracji i Cyfryzacji z dnia 14 sierpnia 2014 r. w sprawie ustalenia regulaminu organizacyjnego Ministerstwa Administracji i Cyfryzacji (Dz. Urz. MAiC z 2014 r., poz. 15).

W latach 2012-2014¹⁷, łączna kwota wydatków poniesionych na zakup sprzętu i oprogramowania wykorzystywanych do ochrony wewnętrznych sieci i systemów teleinformatycznych MAiC wyniosła 666,2 tys. zł. Z udzielonych wyjaśnień wynika, że wydatki związane z bezpieczeństwem IT nie są wydzielane i odrębnie wykazywane w ewidencji księgowej Ministerstwa.

(dowód: akta kontroli tom I str. 383-476)

Ustalone
nieprawidłowości

1. Kontrola wykazała, że Minister Administracji i Cyfryzacji nie podjął rzetelnych działań w celu wdrożenia w podległym mu urzędzie systemu realizacji zadań związanych z ochroną cyberprzestrzeni RP, w szczególności:
 - w MAiC nie przypisano zasobów oraz nie zbudowano potencjału kadrowego i merytorycznego adekwatnego do realizacji zadań dotyczących bezpieczeństwa teleinformatycznego państwa. W okresie 2 lat od utworzenia Ministerstwa, ww. zadania były doraźnie wykonywane przez pracowników Gabinetu Politycznego Ministra, a przez większość tego okresu przez jedną osobę – Szefową Gabinetu Politycznego. Dopiero w styczniu 2014 r. wyznaczono komórkę merytoryczną MAiC odpowiedzialną za realizację zadań związanych z ochroną cyberprzestrzeni, natomiast nie była ona przygotowana kadrowo (2 pracowników) ani merytorycznie (m.in. brak osób posiadających specjalistyczną wiedzę w zakresie funkcjonowania i ochrony systemów teleinformatycznych) do pełnienia roli krajowego ośrodka koordynującego i inicjującego działania innych instytucji państwowych w obszarze bezpieczeństwa teleinformatycznego. (Przykładem niewystarczających kwalifikacji w ww. zakresie jest stwierdzone w toku oględzin przesłanie, przez jedną z ww. osób, z wykorzystaniem prywatnej poczty elektronicznej, niezaszyfrowanego pliku, zawierającego dane służbowe o wysokiej wrażliwości, tj. wstępne zestawienie wyników z audytu wewnętrznego dotyczącego bezpieczeństwa systemów IT, przeprowadzonego w 314 jednostkach administracji rządowej). Działania mające na celu wzmocnienie kadrowe komórki organizacyjnej MAiC odpowiadającej za ochronę cyberprzestrzeni zostały podjęte dopiero w trakcie kontroli NIK i polegały one na zatrudnieniu 2 dodatkowych pracowników.

Podsekretarz Stanu w MAiC – Pan Roman Dmowski wskazał, iż powodem 2-letniego opóźnienia w rozpoczęciu budowy struktur przeznaczonych do realizacji zadań związanych z ochroną cyberprzestrzeni był brak wiedzy odnośnie faktycznych zadań Ministerstwa w tym obszarze. Zeznał, iż: *Do momentu przyjęcia Polityki nie było jasne kto pełni wiodącą rolę w obszarze bezpieczeństwa cyberprzestrzeni, różne zadania były realizowane także przez ABW i MSW. (...) Dopiero przyjęcie Polityki jednoznacznie określiło rolę MAiC.*

Odnosnie przyczyn przekazania w styczniu 2014 r. zadań związanych z ochroną cyberprzestrzeni do komórki organizacyjnej, która nie była przygotowana do ich efektywnej realizacji, Minister Administracji i Cyfryzacji wyjaśnił, iż kluczowym powodem było doświadczenie DSI w zakresie współpracy międzynarodowej i w ramach UE. Było to związane z trwającymi pracami nad dyrektywą NIS, która w ocenie Ministra (...) *była najistotniejszym zadaniem z punktu widzenia przyszłego kształtu systemu cyberbezpieczeństwa Polski. (...).*

W ocenie NIK, nie można uznać za zasadne wyjaśnień Kierownictwa MAiC wskazujących, że dopiero przyjęcie *Polityki* zdeterminowało zadania Ministra w zakresie ochrony cyberprzestrzeni. Obowiązki związane z bezpieczeństwem teleinformatycznym państwa wynikają bowiem bezpośrednio z faktu kierowania przez Ministra Administracji i Cyfryzacji działami administracji rządowej

¹⁷ Wg stanu na dzień 20 listopada 2014 r.

informatyzacja i łączność. W związku z powyższym, w momencie utworzenia MAiC, Minister był zobowiązany do wyznaczenia zasobów i struktur organizacyjnych, adekwatnych do realizacji tych zadań. Udzielone wyjaśnienia wskazują natomiast, iż od momentu wyodrębnienia z MSWiA, w MAiC brak było świadomości obowiązków związanych z ochroną cyberprzestrzeni i ich faktycznego zakresu. Zdaniem NIK, obowiązki Ministra w tym obszarze obejmują kompleksowe działania związane z bezpieczeństwem teleinformatycznym i nie mogą ograniczać się jedynie do wdrażania *Polityki* lub implementacji rozwiązań, które w przyszłości zostaną określone przez dyrektywę NIS;

- do końca okresu objętego kontrolą Kierownictwo MAiC nie oszacowało jakie zasoby (ludzkie, rzeczowe i finansowe) są potrzebne do efektywnej realizacji zadań Ministra Administracji i Cyfryzacji związanych z ochroną cyberprzestrzeni. Podsekretarz Stanu w MAiC wyjaśnił, iż *Podstawową determinantą, na podstawie której dokonano szacowania zasobów ludzkich niezbędnych do skutecznej realizacji zadań MAiC związanych z ochroną cyberprzestrzeni RP była wysokość środków finansowych przeznaczonych na wynagrodzenia. Można wobec tego powiedzieć, że oszacowano raczej zadania, które MAiC jest w stanie wykonywać, mając do dyspozycji ograniczone zasoby. W związku z kategorię sprzeciwem Ministerstwa Finansów wobec zwiększania wydatków budżetu Państwa na realizację polityki cyberbezpieczeństwa, środki obecnie posiadane wyznaczają limit możliwości MAiC. Należy również wskazać, że szacowanie stanu docelowego, tzn. stanu zatrudnienia koniecznego do realizacji zadań MAiC, będzie musiało zostać przeprowadzone z chwilą przyjęcia Dyrektywy NIS i podjęcia decyzji dotyczących sposobu jej wdrożenia do krajowego porządku prawnego. Od tych decyzji będzie bowiem zależało jaką rolę w systemie pełnić będzie MAiC i jakie zasoby ludzkie są konieczne do jej wypełnienia;*
- od momentu utworzenia MAiC w listopadzie 2011 r. do sierpnia 2014 r., tj. do czasu wprowadzenia obowiązującego obecnie regulaminu organizacyjnego Ministerstwa, zadania związane z ochroną cyberprzestrzeni były powierzone w sposób nieformalny, najpierw pracownikom Gabinetu Politycznego, a następnie pracownikom DSI. Pierwszą osobą, której we wrześniu 2013 r. oficjalnie przypisano obowiązki związane z bezpieczeństwem teleinformatycznym był Podsekretarz Stanu nadzorujący realizację tych zadań¹⁸. Brak formalnego wskazania komórki merytorycznej odpowiadającej za ochronę cyberprzestrzeni utrudniał współpracę i wymianę informacji z innymi instytucjami państwowymi wykonującymi zadania w tym zakresie oraz wpłynął negatywnie na realizację zadań Ministerstwa bezpośrednio związanych z bezpieczeństwem teleinformatycznym państwa, np. dotyczących zarządzania kryzysowego (szczegółowo opisano na str. 21-22 i 31-32 wystąpienia pokontrolnego). Podsekretarz Stanu w MAiC wyjaśnił, że zwłoka w formalnym przypisaniu zadań DSI wynikała m.in. z przedłużających się prac nad nowym statutem Ministerstwa;
- nieformalny charakter działań związanych z bezpieczeństwem cyberprzestrzeni w pierwszych latach funkcjonowania Ministerstwa, skutkował brakiem ciągłości w realizacji zadań w tym zakresie. Od momentu przejęcia zadań w styczniu 2014 r. przez DSI, większość działań związanych z ochroną cyberprzestrzeni została rozpoczęta całkowicie od nowa – m.in. jednym z pierwszych zadań pracowników i Kierownictwa ww. Departamentu była analiza treści *Polityki*. Nie kontynuowano części zadań rozpoczętych wcześniej przez Gabinet Polityczny

¹⁸ Od lutego 2014 r. przedmiotowe zadania były wpisywane do zakresów czynności kolejnych pracowników DSI, natomiast ich formalne przypisanie do kompetencji Departamentu nastąpiło z dniem 14 sierpnia 2014 r. na podstawie nowego regulaminu organizacyjnego Ministerstwa.

Ministra we współpracy z Zespołem zadaniowym do spraw ochrony portali rządowych, np. w zakresie monitorowania wydanych przez ABW wytycznych bezpieczeństwa IT dla urzędów administracji rządowej. Należy w szczególności podkreślić, że pracownicy DSI oraz Członek Kierownictwa Ministerstwa odpowiadający za realizację *Polityki* nie mieli wiedzy o trwających w ABW pracach związanych z przygotowaniem metodyki szacowania ryzyka wymaganej na podstawie pkt 3.1. tego dokumentu. W związku z powyższym zamówiono w pośpiechu, z wyłączeniem obowiązujących w MAiC procedur udzielania zamówień publicznych, metodykę sporządzoną przez podmiot zewnętrzny (opisano na str. 22-23 wystąpienia pokontrolnego).

(dowód: akta kontroli tom I str. 4-40, 69-75, 124-152, 376-382, tom III str. 139-180, 391-419, 464-476)

2. W MAiC nie podjęto rzetelnych działań w celu oszacowania zasobów (ludzkich, rzeczowych i finansowych) niezbędnych do skutecznej realizacji zadań związanych z ochroną cyberprzestrzeni RP. W Ministerstwie nie sporządzano analiz/kalkulacji, itp. będących próbą oszacowania tych zasobów oraz nie dysponowano wiedzą na temat potrzeb i zasobów będących w dyspozycji poszczególnych podmiotów zaangażowanych w ochronę bezpieczeństwa teleinformatycznego państwa. Ustalono, iż podmioty administracji rządowej nie realizowały obowiązków wynikających z pkt 5. *Polityki*, dotyczących przekazania Ministrowi Administracji i Cyfryzacji informacji na temat wydatków poniesionych w latach ubiegłych i planowanych na lata 2014-2015 w związku z ochroną cyberprzestrzeni¹⁹. Dane dotyczące zasobów niezbędnych do realizacji tych zadań nie zostały również przekazane w związku z prowadzonymi w MAiC pracami nad przygotowaniem *Planu działań w zakresie zapewnienia bezpieczeństwa cyberprzestrzeni Rzeczypospolitej Polskiej*. Pomimo nieotrzymania przedmiotowych informacji, Minister Administracji i Cyfryzacji nie podjął żadnych działań monitorujących w celu wyegzekwowania realizacji obowiązków określonych w pkt 5. *Polityki*. Nie wydał również wytycznych dotyczących sposobu realizacji tych obowiązków, w szczególności w zakresie sposobów ewidencjonowania i szacowania wydatków na ochronę cyberprzestrzeni. Z ustaleń kontroli wynika natomiast, że w MAiC oraz w innych podmiotach państwowych nie ma możliwości precyzyjnego określenia wysokości wydatków na ochronę cyberprzestrzeni, ponieważ nie są one odrębnie oznaczane i wykazywane w ewidencji księgowej.

Z udzielonych wyjaśnień wynika, że nie realizowano zadań związanych z szacowaniem zasobów i wdrażaniem pkt 5. *Polityki*, z powodu niewystarczającej liczby pracowników DSI dedykowanych do realizacji zadań związanych z ochroną cyberprzestrzeni. Podsekretarz Stanu w MAiC – Pan Roman Dmowski zeznał: *Chciałbym zwrócić uwagę, że realizacja Polityki powinna być prowadzona etapami. Pierwszym etapem jest zwiększenie poziomu świadomości w zakresie cyberbezpieczeństwa, który uruchomi działania na poziomie poszczególnych urzędów. W rezultacie tych działań urzędy będą w stanie określić obszary działań i interwencji, mających na celu podniesienie poziomu bezpieczeństwa. W efekcie zostaną określone konkretne cele i będzie można określić konkretne potrzeby finansowe. Dopiero wtedy będzie możliwa realizacja zapisów pkt 5 i 6 Polityki. (...)*

(dowód: akta kontroli tom I str. 383-396, tom III str. 334-345, 464-474, tom IV str. 252-255, 372-460)

¹⁹ Wymagane informacje zostały przekazane przez Urząd Komunikacji Elektronicznej.

Uwagi dotyczące
badanej działalności

Odpowiedzialność za opisane powyżej nieprawidłowości ponoszą osoby zajmujące w latach 2011 – 2014 stanowisko Ministra Administracji i Cyfryzacji oraz Pan Roman Dmowski – Podsekretarz Stanu w MAiC, któremu od września 2013 r. powierzono zadania związane z ochroną cyberprzestrzeni RP.

NIK zwraca uwagę, iż pomimo podjętych dotychczas działań, zasoby Ministerstwa nie są wystarczające do realnego wykonywania zadań w zakresie koordynacji i inicjowania działań instytucji państwowych związanych z bezpieczeństwem teleinformatycznym oraz koordynacji krajowego systemu reagowania na incydenty komputerowe w cyberprzestrzeni RP (ocena realizacji zadań Ministra w tym zakresie została zawarta w pkt III.3. wystąpienia pokontrolnego). Biorąc pod uwagę stanowisko MF, dotyczące braku akceptacji dodatkowych wydatków na ochronę cyberprzestrzeni, zdaniem NIK, istnieje pilna potrzeba poinformowania Prezesa Rady Ministrów o faktycznych uwarunkowaniach i utrudnieniach w realizacji obowiązków Ministra Administracji i Cyfryzacji oraz podjęcia kluczowych decyzji na szczeblu Rady Ministrów. Jednocześnie należy podkreślić, że podstawą decyzji w ww. zakresie musi być rzetelne i kompleksowe oszacowanie zasobów potrzebnych do budowy krajowego systemu ochrony cyberprzestrzeni, w tym także zadań i zasobów MAiC niezbędnych do ich realizacji.

NIK zwraca również uwagę, iż przez ponad rok od wejścia w życie *Polityki*, w MAiC nie został powołany *Pełnomocnik do spraw bezpieczeństwa cyberprzestrzeni*. Brak działań w tym zakresie wyjaśniano m.in. wątpliwościami dotyczącymi jego właściwego usytuowania w strukturze Ministerstwa. Działania mające na celu ustanowienie Pełnomocnika zostały podjęte dopiero po otrzymaniu pisma kontrolującego w ww. sprawie, co może świadczyć o nieprzypisaniu, przez Kierownictwo MAiC, odpowiedniego priorytetu wdrażaniu postanowień *Polityki* w podległym urzędzie.

Kontrola wykazała, że w MAiC nie została dotychczas zorganizowana odrębna komórka organizacyjna odpowiadająca za bezpieczeństwo wewnętrznych systemów teleinformatycznych. Biorąc pod uwagę szczególną rolę Ministra Administracji i Cyfryzacji w propagowaniu rozwiązań w zakresie bezpieczeństwa IT, jak i wynikające z niej ryzyko skierowania przeciw MAiC ataków, zdaniem NIK, zasadne jest podjęcie działań w celu zorganizowania wewnętrznego zespołu reagowania na incydenty komputerowe.

1.3. Określenie ram prawnych systemu ochrony cyberprzestrzeni.

W *Polityce* nie zawarto propozycji zmian legislacyjnych niezbędnych do stworzenia krajowego systemu ochrony cyberprzestrzeni RP. W pkt 3.3. ww. dokumentu wskazano natomiast, że: *Podstawowym elementem realizacji Polityki, przewidzianym niezwłocznie do wykonania, są działania legislacyjne. Rada Ministrów, rozumiejąc wysoki priorytet tych działań, widzi potrzebę ich zainicjowania przez ministra właściwego ds. informatyzacji, aby stworzyć regulacje prawne, dające podstawy do podejmowania dalszych działań w ramach wdrożenia zapisów Polityki. Konieczny jest przegląd obecnie obowiązujących regulacji prawnych mających na względzie przygotowanie rozwiązań w celu zwiększenia poczucia bezpieczeństwa nie tylko instytucji rządowych ale wszystkich użytkowników cyberprzestrzeni.*

W okresie od utworzenia Ministerstwa, w MAiC opracowano następujące regulacje prawne związane z ochroną cyberprzestrzeni RP:

- decyzję Przewodniczącego Komitetu Rady Ministrów do spraw Cyfryzacji Nr 1/2012 z dnia 24 stycznia 2012 r. w przedmiocie powołania Zespołu zadaniowego do spraw ochrony portali rządowych;

- projekt zarządzenia Prezesa Rady Ministrów w sprawie powołania Zespołu do spraw koordynacji działań związanych z bezpieczeństwem cyberprzestrzeni Rzeczypospolitej Polskiej;
- decyzję Przewodniczącego Komitetu Rady Ministrów do spraw Cyfryzacji Nr 1/2014 z dnia 13 czerwca 2014 r. w sprawie powołania Zespołu zadaniowego do spraw bezpieczeństwa cyberprzestrzeni Rzeczypospolitej Polskiej.
(dowód: akta kontroli tom I str. 4-56, tom IV str. 296-366)

W kwietniu 2014 r., w ramach realizacji obowiązku określonego w art. 175b ust. 4 Prawa telekomunikacyjnego²⁰, przekazany został Ministrowi Administracji i Cyfryzacji Raport Prezesa Urzędu Komunikacji Elektronicznej (UKE) o zgłoszonych w 2013 r. zagrożeniach i podjętych przez przedsiębiorców telekomunikacyjnych działaniach zapobiegawczych i środkach naprawczych w zakresie bezpieczeństwa lub integralności sieci lub informacji. W konkluzjach do Raportu wskazano m.in., iż w ocenie UKE, ustalona w Prawie telekomunikacyjnym zasada, że ocena istotności naruszenia bezpieczeństwa lub integralności sieci lub usług należy do przedsiębiorców, skutkuje fakultatywnością zgłoszeń i powoduje różnorodność kryteriów oceny zdarzeń stosowanych przed przedsiębiorców. Zgodnie z oceną Prezesa UKE, zmiany wymaga art. 175a ust. 1 ustawy Prawo telekomunikacyjne poprzez nałożenie na przedsiębiorców bezwzględnego obowiązku informowania o naruszeniach według określonego kryterium (progów zgłoszeń). W opinii UKE celowe byłoby również wypracowanie jednej, wspólnej dla wszystkich przedsiębiorców metody szacowania liczby użytkowników dotkniętych naruszeniem.

Proponowane przez UKE zmiany Działu VIIa Prawa telekomunikacyjnego zostały ujęte w opracowanym w MAiC projekcie *Planu działań w zakresie zapewnienia bezpieczeństwa cyberprzestrzeni RP*. W Ministerstwie nie przygotowano natomiast projektu nowelizacji ww. przepisów Prawa telekomunikacyjnego.

Podsekretarz Stanu w MAiC – Pan Roman Dmowski zeznał: *Nie mam wiedzy na jakim etapie są prace nad zamianą tego aktu prawnego, ponieważ są one prowadzone w Departamencie Telekomunikacji. Podległe mi komórki organizacyjne nie występowały dotychczas z inicjatywą zmian legislacyjnych w tym obszarze, co wynika z podziału kompetencji między Departamentami. W obszarze bezpieczeństwa cyberprzestrzeni zainicjowaliśmy działania mające na celu umieszczenie tego zadania w Planie działań. Zeznał, że nie weryfikowano działań prowadzonych w tym obszarze przez Departament Telekomunikacji, ponieważ: Plan działań nie jest związany z pracami legislacyjnymi prowadzonymi w tym zakresie w innych komórkach Ministerstwa. (...).*

Zastępca Dyrektora Departamentu Telekomunikacji MAiC – Pan Dariusz Dąbek poinformował, iż w Departamencie Telekomunikacji nie opracowano projektu nowelizacji Prawa telekomunikacyjnego w zakresie postulowanym przez Prezesa UKE. Wyjaśnił, że nie dostrzega konieczności zmiany ww. przepisów, ponieważ w jego opinii, od dnia wejścia w życie przepisu art. 175a ust. 1 ustawy Prawo telekomunikacyjne, istnieje obowiązek zgłaszania naruszeń przez przedsiębiorców. Wskazał również, że przedstawione przez Prezesa UKE propozycje zmian ww. przepisów można uznać za dyskusyjne i nie w pełni uzasadnione, a jednocześnie bardzo trudne do wypracowania i w efekcie do wprowadzenia.

(dowód: akta kontroli tom III str. 354-376, 464-476)

W okresie od utworzenia Ministerstwa, Departament Prawny MAiC uczestniczył w uzgodnieniach treści projektów ustaw o Agencji Bezpieczeństwa Wewnętrznego

²⁰ Ustawa z dnia 16 lipca 2004 r. Prawo telekomunikacyjne (Dz. U. z 2014 r., poz. 243).

i Agencji Wywiadu. Z udzielonych wyjaśnień wynika, że poza ww. ustawą, w okresie objętym kontrolą, Minister Administracji i Cyfryzacji nie uczestniczył²¹ w pracach legislacyjnych prowadzonych przez inne podmioty, mających na celu wprowadzenie do polskiego porządku prawnego zagadnień związanych z cyberprzestrzenią RP.

(dowód: akta kontroli tom I str. 4-56, 383-396)

Ustalone
nieprawidłowości

Kontrola wykazała, że Minister Administracji i Cyfryzacji nie podjął rzetelnych działań w celu realizacji pkt 3.3. *Polityki* dotyczącego działań legislacyjnych. Nie przeprowadzono kompleksowej inwentaryzacji obowiązujących w Polsce aktów prawnych związanych z bezpieczeństwem teleinformatycznym, nie określono pożądanych kierunków zmian legislacyjnych oraz nie przygotowano żadnych projektów aktów prawnych (poza wewnętrznymi regulacjami dotyczącym powołania zespołów międzyresortowych) w zakresie budowy krajowego systemu ochrony cyberprzestrzeni. W przypadku zgłoszonej przez UKE inicjatywy zmiany Prawa telekomunikacyjnego, nie wypracowano wspólnego stanowiska między właściwymi merytorycznie komórkami organizacyjnymi MAiC. Z wyjaśnień udzielonych przed Podsekretarza Stanu w MAiC – Pana Romana Dmowskiego wynika, że na obecnym etapie, ze względu na trwające prace nad dyrektywą NIS, podjęcie działań legislacyjnych w celu budowy krajowego systemu ochrony cyberprzestrzeni byłoby przedwczesne. Zeznał również, iż w jego opinii uzasadnione są nowelizacje istniejących regulacji prawnych dotyczących cyberprzestrzeni (np. Prawa telekomunikacyjnego), natomiast ciałem które powinno wskazywać kierunki tych zmian jest Zespół zadaniowy do spraw bezpieczeństwa cyberprzestrzeni RP.

W ocenie NIK, organem odpowiedzialnym za inicjowanie prac legislacyjnych w obszarze ochrony cyberprzestrzeni jest Minister Administracji i Cyfryzacji. Powyższe wynika zarówno z faktu kierowania działami administracji informatyzacja i łączność, jak i bezpośrednio z zapisów pkt 3.3. *Polityki*. Zdaniem NIK, nie można również uznać wyjaśnień uzasadniających wstrzymanie prac nad krajowym systemem ochrony cyberprzestrzeni, oczekiwaniem na dyrektywę NIS. Biorąc pod uwagę ryzyka związane z ww. aktem prawnym (dotyczące jego zakresu i terminu wejścia w życie) oraz wzrastające uzależnienie realizacji zadań publicznych od funkcjonowania systemów teleinformatycznych, zasadne jest podjęcie kompleksowych działań, w tym legislacyjnych, w celu poprawy bezpieczeństwa IT.

Odpowiedzialność za opisane powyżej nieprawidłowości ponoszą osoby zajmujące w latach 2011 – 2014 stanowisko Ministra Administracji i Cyfryzacji oraz Pan Roman Dmowski – Podsekretarz Stanu w MAiC, któremu od września 2013 r. powierzono zadania związane z ochroną cyberprzestrzeni RP.

1.4. Określenie celów, mierników i terminów realizacji zadań związanych z budową systemu ochrony cyberprzestrzeni RP.

W *Polityce* nie określono szczegółowych celów, produktów, mierników oraz terminów realizacji działań związanych z ochroną cyberprzestrzeni RP. Nie dokonano również precyzyjnego podziału zadań między poszczególnych użytkowników i administratorów cyberprzestrzeni. Uzupełnienie ww. dokumentu powinno być dokonane z zastosowaniem procedury opisanej w pkt 6. i 6.3. *Polityki*, obejmującej dwa etapy, tj.:

- opracowanie przez poszczególne podmioty zaangażowane w ochronę cyberprzestrzeni jednostkowych wskaźników realizacji zadań (w ciągu roku od wejścia w życie *Polityki*);

²¹ Do dnia 29 października 2014 r.

- opracowanie przez MAiC globalnych, zagregowanych wskaźników realizacji *Polityki* (po przeprowadzeniu szacowania ryzyka).

Ustalono, iż podmioty administracji rządowej nie realizowały obowiązków wynikających z pkt 6. i 6.3. *Polityki*, dotyczących przekazania Ministrowi Administracji i Cyfryzacji, w ciągu roku od przyjęcia tego dokumentu, informacji na temat przyjętych i osiągniętych wskaźników realizacji zadań związanych z ochroną cyberprzestrzeni²².

(dowód: akta kontroli tom IV str. 252-255)

Ustalone
nieprawidłowości

Minister Administracji i Cyfryzacji nie podjął żadnych działań mających na celu wyegzekwowanie od podmiotów administracji rządowej realizacji obowiązków określonych w pkt 6. i 6.3. *Polityki*. W MAiC nie rozpoczęto również prac zmierzających do przygotowania globalnych, zagregowanych wskaźników realizacji zadań wymienionych w *Polityce*.

Pracownicy DSI wyjaśnili, iż: *Nie podejmowano działań monitorujących w ww. zakresie, ponieważ uwzględniając siły i środki DSI, nie było możliwości przystąpienia do realizacji wszystkich zadań wynikających z Polityki równocześnie. (...) Podjęto decyzję, że mając na uwadze opóźnienia w realizacji Polityki, kluczowe znaczenie miało przystąpienie do realizacji poszczególnych działań, a ocena ich skuteczności została odłożona na etap późniejszy. (...) Należy również zwrócić uwagę, że zadanie dot. koordynacji Polityki zostało przekazane do DSI dopiero w styczniu 2014 r. Nie było przy tym żadnej ciągłości (personalnej i merytorycznej) w realizacji zadań z zakresu bezpieczeństwa cyberprzestrzeni prowadzonych wcześniej przez Gabinet Polityczny Ministra. DSI musiał zbudować wiedzę i kompetencje, w tym instytucjonalne już w trakcie wdrażania Polityki.*

Podsekretarz Stanu w MAiC – Pan Roman Dmowski zeznał: *Chciałbym zwrócić uwagę, że realizacja Polityki powinna być prowadzona etapami. (...) moment, w którym powstanie Plan działań, będzie właściwy aby stworzyć mierniki, które pozwolą ocenić skuteczność realizacji Planu i tym samym Polityki.*

(dowód: akta kontroli tom III str. 466-474, tom IV str. 252-255)

Odpowiedzialność za opisane powyżej nieprawidłowości ponoszą osoby zajmujące w latach 2013 – 2014 stanowisko Ministra Administracji i Cyfryzacji oraz Pan Roman Dmowski – Podsekretarz Stanu w MAiC, któremu od września 2013 r. powierzono zadania związane z ochroną cyberprzestrzeni RP.

1.5. Opracowanie projektów szczegółowych określających sposób realizacji *Polityki*.

Zgodnie z zapisami *Polityki*, określone w tym dokumencie działania w zakresie ochrony cyberprzestrzeni miały być realizowane w formie tzw. *projektów szczegółowych*. W szczególności, w *Polityce* przewidziano następujące projekty szczegółowe: pkt 3.4. – działania proceduralno-organizacyjne, pkt 3.6. – działania techniczne, pkt 3.6.1. – realizacja projektów badawczych, pkt. 3.6.3. – rozbudowa systemu wczesnego ostrzegania ARAKIS, pkt 4. – projekty szczegółowe dotyczące celów i założeń *Polityki*.

W MAiC nie zostały opracowane żadne projekty szczegółowe dotyczące wdrażania działań przewidzianych w *Polityce*. Kierownictwo Ministerstwa nie dysponowało

²² Wymagane informacje zostały przekazane przez Rządowe Centrum Bezpieczeństwa.

również wiedzą, jakie projekty szczegółowe są realizowane przez inne podmioty zobowiązane do wdrażania *Polityki* oraz jaki jest ich cel i zakres²³.

Podsekretarz Stanu w MAiC – Pan Roman Dmowski wyjaśnił, iż „*Polityka ochrony cyberprzestrzeni RP*” nie zawiera wytycznych – odmiennie jak projekt „*Rządowego Programu Ochrony Cyberprzestrzeni RP*” – jak winny być opracowane projekty szczegółowe, co może oznaczać, że koncepcja projektu szczegółowego to domena podmiotów realizujących projekt. Jak wskazano poprzednio Zespół zadaniowy ds. bezpieczeństwa cyberprzestrzeni określi wytyczne odnośnie projektów szczegółowych.

(dowód: akta kontroli tom I str. 4-40, 270-281, tom III str. 470)

Uwagi dotyczące
badanej działalności

NIK zwraca uwagę, iż w związku z nieprecyzyjnym brzmieniem zapisów *Polityki* istnieje potrzeba podjęcia pilnych decyzji odnośnie ram organizacyjnych wdrażania tego dokumentu, w tym zakresu, formy i podmiotów odpowiedzialnych za realizację projektów szczegółowych. Należy jednocześnie podkreślić, że zgodnie z pkt 1.5. *Polityki*, podmiotem koordynującym realizację tego dokumentu jest Minister Administracji i Cyfryzacji, który powinien inicjować działania związane z ochroną cyberprzestrzeni oraz monitorować sposób wykonania tych zadań przez poszczególne instytucje państwowe.

1.6. Ustanowienie kanałów wymiany informacji oraz krajowego systemu reagowania na incydenty komputerowe.

W MAiC nie wypracowano klasyfikacji incydentów komputerowych oraz bazujących na tej klasyfikacji procedur reagowania na poszczególne rodzaje incydentów przeznaczonych dla różnych grup użytkowników oraz podmiotów odpowiadających za ochronę cyberprzestrzeni. W trakcie spotkań Zespołu zadaniowego do spraw ochrony portali rządowych rozważano stworzenie wewnętrznego portalu administracji państwowej, który stanowiłby m.in. bazę wiedzy na temat zagrożeń. Przygotowanie wstępnych założeń takiego portalu wraz z procedurami jego obsługi zlecono, w trakcie spotkania Zespołu w dniu 8 maja 2013 r., przedstawicielom MSW, MSZ i ABW, natomiast obecne Kierownictwo MAiC nie dysponowało wiedzą i dokumentacją dotyczącą efektów ww. prac. Od momentu przekazania zadań związanych z ochroną cyberprzestrzeni do DSI, w MAiC nie prowadzono działań związanych z opracowaniem klasyfikacji incydentów komputerowych oraz przypisanych do nich procedur reagowania. Powyższe wyjaśniano ograniczonymi zasobami kadrowymi oraz koniecznością realizacji innych, priorytetowych zadań.

(dowód: akta kontroli tom I str. 153-188, 201-202)

W latach 2012-2013, w ramach prac Zespołu zadaniowego do spraw ochrony portali rządowych, w których uczestniczyli pracownicy Gabinetu Politycznego Ministra Administracji i Cyfryzacji, podjęto działania mające na celu ustanowienie mechanizmów wymiany informacji między podmiotami państwowymi w zakresie incydentów komputerowych. W ramach realizacji zaleceń ww. Zespołu, w MAiC zabrano dane kontaktowe wskazanych w poszczególnych ministerstwach i urzędach wojewódzkich 2 pracowników, do których zadań przypisano kontakty z Rządowym Zespołem Reagowania na Incydenty Komputerowe CERT.GOV.PL i informowanie o incydentach.

(dowód: akta kontroli tom I str. 237-265)

W MAiC nie podejmowano działań w celu wypracowania specyficznych procedur łączności wspomagających funkcjonowanie krajowego systemu reagowania

²³ Z ustaleń kontroli wynika, że jedynym projektem szczegółowym realizowanym dotychczas na podstawie *Polityki* jest, wdrażany przez ABW oraz przez Narodową i Akademicką Sieć Komputerową, projekt dotyczący wytworzenia i rozbudowy systemu wczesnego ostrzegania ARAKIS.

na incydenty komputerowe w cyberprzestrzeni RP, określonego w pkt 4.2 *Polityki*. Kierownictwo MAiC nie dysponowało również wiedzą, w jaki sposób krajowy system reagowania na incydenty komputerowe zapewnia wymianę informacji pomiędzy zespołami administracji publicznej oraz zespołami CERT²⁴ i innymi komercyjnymi użytkownikami i administratorami cyberprzestrzeni wymienionymi w pkt 4.2 *Polityki*, ani czy system ten spełnia wymagania określone w pkt 4.3 *Polityki*.

Podsekretarz Stanu w MAiC - Pan Roman Dmowski wyjaśnił m.in., iż: MAiC (...) *nie pełni roli operacyjnej w zakresie zapewniania bezpieczeństwa cybernetycznego, nie jest więc w stanie określić (...) w jaki sposób wymieniane są informacje pomiędzy zespołami administracji publicznej oraz zespołami CERT i innymi komercyjnymi użytkownikami i administratorami cyberprzestrzeni (...) i czy system ten działa w sposób w pełni prawidłowy. (...) Punkt 4.3 zakłada wymianę informacji pozyskanych we współpracy międzynarodowej pomiędzy zespołami rządowymi, wojskowymi i cywilnymi typu CERT, co może oznaczać, że mechanizm wymiany informacji dotyczyć będzie zarówno bieżącej współpracy operacyjnej zespołów CERT oraz współpracy bardziej o charakterze politycznym (...) MAiC nie posiada jednak szczegółowych informacji co do skuteczności obiegu informacji uzyskiwanej w ten sposób. Postanowienia punktu 4.3 Polityki są też niezwykle lakoniczne i nie jest jasne, w jaki sposób „system” miałby określać np. alternatywne kanały wymiany informacji, ani nawet czym te kanały są.*

(dowód: akta kontroli tom I str. 153-183)

Uwagi dotyczące
badanej działalności

NIK zwraca uwagę, iż poza opisanymi powyżej działaniami pracowników Gabinetu Politycznego, Minister Administracji i Cyfryzacji nie realizował praktycznie żadnych zadań w zakresie budowy krajowego systemu reagowania na incydenty komputerowe. Stwierdzono również, iż m.in. w związku z wątpliwościami interpretacyjnymi dotyczącymi pkt 4.2. i 4.3. *Polityki*, w MAiC nie określono w sposób precyzyjny, jakie zadania powinny być realizowane przez Ministra w związku z budową tego systemu. Zdaniem NIK, wdrożenie skutecznych mechanizmów wymiany informacji o incydentach ma kluczowe znaczenie dla funkcjonowania systemu ochrony cyberprzestrzeni RP, a odpowiedzialność za realizację tego zadania ponosi Minister Administracji i Cyfryzacji, jako podmiot koordynujący krajowy system reagowania na incydenty komputerowe.

1.7. Koordynacja systemu ochrony cyberprzestrzeni RP.

Zgodnie z pkt 3.4.1. *Polityki*: *W ramach zarządzania bezpieczeństwem cyberprzestrzeni RP, a także w celu usprawnienia procesu realizacji celów Polityki oraz zapewnienia skuteczności działań organów władzy państwowej w zakresie bezpieczeństwa CRP jest niezbędne powołanie przez Prezesa Rady Ministrów zespołu odpowiedzialnego za przygotowywanie rekomendacji z zakresu wykonania czy koordynacji wszelkich działań związanych z jej bezpieczeństwem (zwanego dalej Zespołem). (...) Zaleca się, aby Zespół, w terminie 30 dni od dnia powołania, przygotował i przedstawił plan działań w zakresie zapewnienia bezpieczeństwa cyberprzestrzeni RP.*

W MAiC został przygotowany i przekazany w dniu 20 listopada 2013 r. Sekretarzowi Stałego Komitetu Rady Ministrów²⁵, projekt zarządzenia Prezesa Rady Ministrów w sprawie powołania Zespołu do spraw koordynacji działań związanych z bezpieczeństwem cyberprzestrzeni Rzeczypospolitej Polskiej. Przedmiotowy projekt zakładał m.in. przedstawianie Radzie Ministrów wyników prac Zespołu oraz okresowe składanie Radzie Ministrów sprawozdań z realizacji zadań. Pismem z dnia

²⁴ Zespół reagowania na incydenty komputerowe – ang. Computer Emergency Response Team.

²⁵ Projekt zarządzenia został uzgodniony międzyresortowo i przyjęty przez Komitet Rady Ministrów do spraw Cyfryzacji.

10 stycznia 2014 r. Sekretarz Stałego Komitetu Rady Ministrów zwróciła ww. projekt do MAiC wskazując, że: *powyższe wynika z ustaleń poczynionych przez Przewodniczącego Stałego Komitetu Rady Ministrów z Panem Rafałem Trzaskowskim, Ministrem Administracji i Cyfryzacji.*

(dowód: akta kontroli tom IV str. 296-352)

Obecne Kierownictwo MAiC nie dysponowało wiedzą, ani dokumentacją pozwalającą na ustalenie przyczyn rezygnacji z powołania ww. Zespołu. Podsekretarz Stanu w MAiC – Pan Roman Dmowski zeznał: *Nie mam precyzyjnej wiedzy na ten temat. W mojej ocenie kluczowa w tej kwestii była dyskusja podczas posiedzenia Komitetu Stałego Rady Ministrów. Przypuszczam, że ta decyzja wynikała z przekonania, że utworzenie Zespołu w ramach Komitetu Rady Ministrów ds. Cyfryzacji zapewni największą efektywność działań tego Zespołu.*

Na zadane w tej sprawie Prezesowi Rady Ministrów pytanie odpowiedział Szef Kancelarii Prezesa Rady Ministrów – Pan Jacek Cichocki, który wyjaśnił, że na podstawie ustaleń poczynionych przez Przewodniczącego Stałego Komitetu Rady Ministrów z ówczesnym Ministrem Administracji i Cyfryzacji przyjęto, że zadania przewidziane dla zespołu ds. koordynacji działań związanych z bezpieczeństwem cyberprzestrzeni mogą być realizowane przez Komitet Rady Ministrów ds. Cyfryzacji. W związku z powyższym powoływanie kolejnego organu pomocniczego, jakim byłby ww. zespół, nie byłoby racjonalne. Wpisywało się to także w zalecenia Prezesa Rady Ministrów dotyczące konieczności przeglądu zespołów międzyresortowych pod kątem zasadności ich funkcjonowania.

(dowód: akta kontroli tom I str. 383-396, 464-474, tom III str. 466-474, 481-484)

Kierownictwo MAiC nie podejmowało dalszych działań w celu zmiany ww. decyzji i powołania Zespołu przewidzianego w pkt 3.4.1. *Polityki*. W miejsce ww. Zespołu, w dniu 13 czerwca 2014 r. powołany został *Zespół zadaniowy do spraw bezpieczeństwa cyberprzestrzeni Rzeczypospolitej Polskiej*²⁶, będący zespołem zadaniowym Komitetu Rady Ministrów do spraw Cyfryzacji²⁷. Do zadań Zespołu należało w szczególności:

1. Przygotowanie, w terminie 3 miesięcy od daty powołania Zespołu, tj. do dnia 13 września 2014 r., *Planu działań w zakresie zapewnienia bezpieczeństwa cyberprzestrzeni RP* – w decyzji nie określono komu ww. plan ma zostać przekazany oraz w jaki sposób ma przebiegać jego wdrażanie. Naczelnik Wydziału Unii Europejskiej i Spraw Międzynarodowych DSI – Pan Marcin Olender wyjaśnił, że *plan powinien być realizowany pod koordynacją MAiC, natomiast nie będzie on miał charakteru wiążącego dla instytucji publicznych. Jego realizacja będzie zależała od zgodnego współdziałania członków Zespołu.*
2. Opracowanie propozycji działań dla jednostek administracji rządowej, mających na celu ochronę systemów teleinformatycznych i usług funkcjonujących w ramach tych systemów przed cyberatakami.
3. Opracowanie propozycji standardów bezpieczeństwa dla systemów teleinformatycznych jednostek administracji rządowej i usług funkcjonujących w ramach tych systemów.

²⁶ Na podstawie Decyzji Przewodniczącego Komitetu Rady Ministrów do spraw Cyfryzacji Nr 1/2014 z dnia 13 czerwca 2014 r.

²⁷ W skład Zespołu weszli: Minister Administracji i Cyfryzacji, Minister Spraw Wewnętrznych (współprzewodniczący Zespołu), Minister Infrastruktury i Rozwoju oraz członkowie Komitetu Rady Ministrów do spraw Cyfryzacji z następujących resortów: Ministerstwa Edukacji Narodowej, Ministerstwa Finansów, Ministerstwa Gospodarki, Ministerstwa Infrastruktury i Rozwoju, Ministerstwa Nauki i Szkolnictwa Wyższego, Ministerstwa Obrony Narodowej, Ministerstwa Sprawiedliwości, Ministerstwa Spraw Zagranicznych, Ministerstwa Zdrowia, Ministerstwa Spraw Wewnętrznych, Ministerstwa Administracji i Cyfryzacji. W pracach Zespołu mogą brać udział, z głosem doradczym, inne osoby zaproszone przez Przewodniczącego.

4. Koordynowanie działań instytucji realizujących zadania wynikające z *Polityki*.

Termin realizacji zadań wymienionych w pkt 2-3 został wyznaczony na dzień 13 grudnia 2014 r. Zgodnie z § 5 ust. 2 ww. decyzji, posiedzenia Zespołu powinny się odbywać nie rzadziej, niż raz na trzy miesiące.

(dowód: akta kontroli tom IV str. 353-366)

Podsekretarz Stanu w MAiC – Pan Roman Dmowski zeznał, iż w jego ocenie umiejscowienie Zespołu przy Komitecie Rady Ministrów do spraw Cyfryzacji jest optymalne a możliwości jego oddziaływania są porównywalne z możliwościami Zespołu przewidzianego w pkt 3.4.1 *Polityki*.

(dowód: akta kontroli tom III str. 466-474)

Wg stanu na dzień zakończenia kontroli, odbyło się jedno posiedzenie *Zespołu zadaniowego do spraw bezpieczeństwa cyberprzestrzeni RP* – w dniu 28 lipca 2014 r.²⁸. W wyniku dokonanych uzgodnień, podmioty uczestniczące w pracach Zespołu zostały zobowiązane do przekazania do MAiC, do końca sierpnia 2014 r., wkładów do *Planu działań w zakresie zapewnienia bezpieczeństwa cyberprzestrzeni RP*, zawierających informacje o:

- proponowanych działaniach w celu zapewnienia bezpieczeństwa cyberprzestrzeni;
- podmiotach odpowiadających za realizację działań;
- terminie realizacji działań (w ramach horyzontu czasowego 2-3 lat);
- zasobach (ludzkich, technicznych i finansowych do realizacji działań).

Analiza dokumentacji przekazanej przez instytucje uczestniczące w pracach Zespołu wykazała, że część podmiotów²⁹:

- nie wywiązała się z obowiązku przekazania wkładu do MAiC (Minister Edukacji Narodowej, Generalny Inspektor Ochrony Danych Osobowych);
- przekazała dane odnoszące się wyłącznie do wewnętrznych systemów teleinformatycznych, bez uwzględnia wkładu tych instytucji w krajowy system ochrony cyberprzestrzeni (Minister Spraw Wewnętrznych, Minister Sprawiedliwości, Komendant Główny Policji, Minister Zdrowia);
- przekazała wkład w innej szczegółowości niż wymagana przez MAiC (np. Dyrektor Narodowego Centrum Kryptologii) lub nie przekazała wszystkich wymaganych informacji (w większości przypadków nie określono precyzyjnie zasobów ludzkich, finansowych i rzeczowych niezbędnych do realizacji zadań).

Naczelnik Wydziału Unii Europejskiej i Spraw Międzynarodowych DSI wyjaśnił, że nie podejmowano działań monitorujących wobec podmiotów, które nie przekazały wkładów do Planu, lub przekazały niepełne informacje, ponieważ oczekiwano na uzupełnianie informacji. Wskazał, że MAiC dysponuje wystarczającą liczbą materiału do opracowania wstępnej wersji planu. Jak wyjaśnił: *Zakładamy, że przedstawienie projektu planu Zespołowi wywoła dyskusję oraz spowoduje uzupełnienie i modyfikację tego dokumentu.*

W MAiC opracowano projekt *Planu działań w zakresie zapewnienia bezpieczeństwa cyberprzestrzeni RP*, który został przekazany w dniu 17 listopada 2014 r. do konsultacji podmiotom uczestniczącym w pracach *Zespołu zadaniowego do spraw bezpieczeństwa cyberprzestrzeni Rzeczypospolitej Polskiej*. Ww. projekt miał zostać rozpatrzony na drugim posiedzeniu Zespołu zaplanowanym na dzień 8 grudnia 2014 r.

²⁸ Kolejne posiedzenie zostało zwołane na dzień 8 grudnia 2014 r.

²⁹ Wg stanu na dzień 10 października 2014 r.

Odnosnie opóźnienia w przygotowaniu Planu w stosunku do terminu wynikającego z decyzji powołującej Zespół (13 września 2014 r.) Naczelnik Wydziału Unii Europejskiej i Spraw Międzynarodowych DSI wyjaśnił, że: *uwzględniając datę pierwszego spotkania zespołu (28 lipca 2014 r.) oraz czas wyznaczony na przekazanie wkładów przez członków Zespołu, wskazany w ww. decyzji termin był mało realistyczny. Należy też podkreślić, że działania DSI miały na celu przygotowanie kompleksowego, poprawnego merytorycznie planu, a nie dokonanie prostej agregacji otrzymanych wkładów.*

(dowód: akta kontroli tom III str. 354-376, tom IV str. 367-460)

Podsekretarz Stanu w MAiC – Pan Roman Dmowski zeznał, iż w jego ocenie długi okres czasu, który upłynął do pierwszego posiedzenia Zespołu był uzasadniony i służył przygotowaniu kluczowego dokumentu, jakim jest *Plan działań w zakresie zapewnienia bezpieczeństwa cyberprzestrzeni RP.*

(dowód: akta kontroli tom III str. 466-474)

Uwagi dotyczące
badanej działalności

NIK zwraca uwagę, że działania Ministra Administracji i Cyfryzacji w zakresie powołania Zespołu do spraw koordynacji działań związanych z bezpieczeństwem cyberprzestrzeni były nierzetelne. Przedstawiona uwaga wynika przede wszystkim z faktu, iż po zwróceniu przez Sekretarza Stałego Komitetu Rady Ministrów projektu zarządzenia powołującego ww. zespół, Kierownictwo MAiC nie podejmowało żadnych działań mających na celu zmianę tej decyzji i powołanie Zespołu w formie przewidzianej w pkt 3.4.1. *Polityki*. W rezultacie, Minister Administracji i Cyfryzacji (Przewodniczący Komitetu Rady Ministrów do spraw Cyfryzacji), wydał decyzję, która jest niezgodna z uchwałą Rady Ministrów w sprawie przyjęcia *Polityki*, w zakresie formy prawnej Zespołu ds. koordynacji działań związanych z bezpieczeństwem cyberprzestrzeni oraz terminu wyznaczonego na opracowanie Planu działań w zakresie zapewnienia bezpieczeństwa cyberprzestrzeni RP (termin realizacji tego zadania wydłużono o 60 dni). NIK nie podziela również stanowiska Kierownictwa MAiC, iż zmiana formy prawnej Zespołu nie wpłynęła negatywnie na możliwość realizacji zadań w zakresie ochrony cyberprzestrzeni. W ocenie NIK, obniżenie rangi Zespołu, w istotny sposób zmniejszyło możliwość wykorzystania wyników jego prac, które nie będą, jak pierwotnie planowano, przekazywane Radzie Ministrów i będą stanowić tylko niewiążącą rekomendację. Przeniesienie ww. zadań na poziom Komitetu Rady Ministrów do spraw Cyfryzacji ogranicza również udział w realizacji zadań związanych z ochroną cyberprzestrzeni kluczowych decydentów odpowiadających za bezpieczeństwo państwa, tj. Rady Ministrów i Prezesa Rady Ministrów.

NIK zwraca również uwagę, iż dotychczasowe działania związane z budową systemu koordynacji zadań w obszarze ochrony cyberprzestrzeni RP były nieefektywne i realizowane ze znacznym opóźnieniem. Świadczy o tym fakt, iż dopiero po upływie roku od przyjęcia *Polityki*, powołany został Zespół, którego zadaniem jest wspieranie Ministra Administracji i Cyfryzacji w koordynacji ww. zadań, a do końca kontroli odbyło się tylko jedno posiedzenie tego Zespołu. Pomimo wydłużenia terminu określonego w pkt 3.4.1. *Polityki*, do końca kontroli nie zostało zrealizowane pierwsze z zadań ww. Zespołu, tj. nie został przygotowany Plan działań w zakresie zapewnienia bezpieczeństwa cyberprzestrzeni RP. Powyższe, zdaniem NIK, wynikało zarówno z braku przygotowania organizacyjnego i kadrowego MAiC do koordynacji działań związanych z ochroną cyberprzestrzeni (szczegółowo opisano w pkt III.1.1.2. wystąpienia), jak również z problemów we współpracy z innymi podmiotami państwowymi, które powinny realizować zadania z zakresu bezpieczeństwa teleinformatycznego.

Ocena cząstkowa

Najwyższa Izba Kontroli ocenia negatywnie dotychczasową działalność Ministra Administracji i Cyfryzacji w zakresie budowy systemu ochrony cyberprzestrzeni RP.

2. Szacowanie ryzyk związanych ze zdarzeniami występującymi w cyberprzestrzeni.

Opis stanu
faktycznego

Raport o zagrożeniach bezpieczeństwa narodowego.

We wrześniu 2012 r., w ramach realizacji obowiązku wynikającego z art. 5a ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym³⁰, MAiC przekazało do RCB i ABW raport cząstkowy o zagrożeniach bezpieczeństwa narodowego obejmujący działy administracji rządowej kierowane przez Ministra Administracji i Cyfryzacji. W ww. raporcie zagrożenia występujące w cyberprzestrzeni RP³¹ zostały ograniczone do cyberterroryzmu³², a ich potencjalny zasięg oddziaływania odniesiono tylko do sieci teleinformatycznych przedsiębiorców telekomunikacyjnych i operatorów pocztowych. Jednocześnie wskazano, że zagrożenia związane z cyberterroryzmem nie mają bezpośrednich skutków dla gospodarki kraju oraz środowiska naturalnego, a Minister Administracji i Cyfryzacji pełni tylko rolę pomocniczą w zakresie zarządzania tymi zagrożeniami. W raporcie określono poziom ryzyka dla zagrożeń ze strony cyberterroryzmu jako akceptowalny uzasadniając, że: *Istniejące rozwiązania zapewniają właściwą ochronę przed zagrożeniami. (...)*. W związku z zawężającą definicją zagrożeń występujących w cyberprzestrzeni, w kolejnych częściach raportu cząstkowego zawarto ograniczony katalog zadań i zasobów przypisanych do zarządzania tymi zagrożeniami³³. W raporcie nie wskazano żadnych danych historycznych dotyczących incydentów związanych z cyberprzestrzenią, ani wniosków dotyczących poprawy bezpieczeństwa narodowego w tym obszarze. Nie wprowadzono również zmian do ww. raportu cząstkowego, pomimo otrzymania od ABW uwag wskazujących na braki merytoryczne w przyjętej przez MAiC definicji zagrożeń występujących w cyberprzestrzeni oraz na konieczność dostosowania raportu do zapisów opracowanego w MAiC projektu *Polityki*.

Zastępująca Dyrektora Generalnego MAiC – Pani Elżbieta Markowska wyjaśniła, iż sposób przedstawienia w raporcie zagrożeń związanych z cyberprzestrzenią oraz zadań Ministra Administracji i Cyfryzacji wynikał m.in. z faktu niewyznaczenia w Ministerstwie komórki organizacyjnej odpowiadającej za ochronę cyberprzestrzeni. Wskazała również, że: *Raport uwzględniał tylko – z punktu widzenia ministra właściwego ds. łączności zagrożenia cyberterroryzmu mogące wpłynąć na działalność przedsiębiorców telekomunikacyjnych, z uwagi na fakt, że w tym czasie nie był wskazany organ administracji rządowej, który byłby odpowiedzialny za sprawy ochrony cyberprzestrzeni w państwie. Stało się to dopiero z chwilą przyjęcia przez Radę Ministrów w dniu 25 czerwca 2013 r. Polityki Ochrony Cyberprzestrzeni RP.*

(dowód: akta kontroli tom V str. 5-10, 83-94)

Do dnia rozpoczęcia kontroli NIK, w MAiC nie podejmowano żadnych działań w celu zaktualizowania raportu cząstkowego Ministra Administracji i Cyfryzacji o zagrożeniach bezpieczeństwa narodowego, m.in. poprzez wskazanie przykładowych zagrożeń oraz dostosowanie tego dokumentu do zapisów *Polityki*. Podsekretarz Stanu w MAiC – Pan Roman Dmowski wyjaśnił, że: *(...) Po przekazaniu zadań związanych z realizacją Polityki do DSI, pracownicy (...)*

³⁰ Dz. U. z 2013 r., poz. 1166.

³¹ W raporcie wskazano również przykładowe zagrożenia dla jednego z systemów teleinformatycznych (ePUAP) wykorzystywanych do realizacji zadań Ministra Administracji i Cyfryzacji.

³² Z pominięciem innych przykładowych zagrożeń takich jak: cyber-chuligani, cyber-aktywiści, cyber-przestępcy, działalność szpiegowska w sieci, działania zbrojne w cyberprzestrzeni kierowane przez inne państwa, itd.

³³ Zasoby MAiC, UKE, przedsiębiorców telekomunikacyjnych oraz operatorów pocztowych i zadania nałożone na te podmioty na podstawie Prawa telekomunikacyjnego.

przystąpili do realizacji niezbędnych działań w tym przede wszystkim szacowania ryzyka cyberprzestrzeni oraz prac nad dyrektywą UE, gdzie harmonogram prac nie pozwalał na ich odłożenie na termin późniejszy. W konsekwencji nie było możliwości zajęcia się innymi zagadnieniami, leżącymi zasadniczo poza kompetencjami DSI, choć związanymi tematycznie. (...).

(dowód: akta kontroli tom V str. 5-10, 83-119)

W trakcie kontroli NIK, w dniu 30 września 2014 r., Minister Administracji i Cyfryzacji przekazał do RCB zaktualizowany raport częściowy o zagrożeniach bezpieczeństwa narodowego³⁴. W raporcie wskazano m.in.: katalog przykładowych zagrożeń cybernetycznych o znacznym wpływie na bezpieczeństwo państwa oraz przykłady działań zapobiegawczych i podnoszących poziom bezpieczeństwa cyberprzestrzeni.

(dowód: akta kontroli tom V str. 5-10)

Szacowanie ryzyka związanego z funkcjonowaniem cyberprzestrzeni.

Na podstawie pkt 3.1. *Polityki*, jednostki administracji rządowej zostały zobowiązane do przeprowadzania szacowania ryzyka związanego z funkcjonowaniem cyberprzestrzeni oraz do przekazywania wyników tych analiz, do dnia 31 stycznia każdego roku, do MAiC. Podmiotem odpowiadającym za przygotowanie jednolitej metodyki analizy ryzyka był Minister Administracji i Cyfryzacji. *Polityka* zalecała również, aby ABW przygotowała katalogi zagrożeń i podatności związanych z cyberprzestrzenią. Termin przekazania do MAiC wyników szacowania ryzyka, za rok 2013 upłynął w dniu 31 stycznia 2014 r.

W dniu 27 stycznia 2014 r., Dyrektor DSI – Pan Maciej Groń wystąpił z wnioskiem o wyrażenie zgody na zamówienie, z wyłączeniem stosowania wewnętrznych przepisów Ministerstwa dotyczących zamówień publicznych, gotowej metodyki szacowania ryzyka związanego z funkcjonowaniem cyberprzestrzeni. We wniosku wskazano podmiot, któremu planowano udzielić zamówienia, uzasadniając odstąpienie od standardowych procedur specjalistycznym charakterem zamówienia. Przedmiotowy wniosek został zaakceptowany przez Podsekretarza Stanu w MAiC – Pana Romana Dmowskiego oraz przez ówczesnego Ministra Administracji i Cyfryzacji – Pana Rafała Trzaskowskiego.

Z wyjaśnień pracowników DSI wynika, że wybór wykonawcy metodyki został dokonany na podstawie przeprowadzonej analizy wskazującej, że podmiot ten przeprowadził najwięcej projektów w zakresie zarządzania bezpieczeństwem informacji i w obszarze kontroli zarządczej. Jednocześnie wyjaśniono, że nie przeprowadzono w tym zakresie pogłębionej analizy rynku, co wynikało z uzyskanej zgody dotyczącej odstąpienia od stosowania procedur zamówień publicznych.

W dniu 6 lutego 2014 r. została podpisana umowa, której przedmiotem było opracowanie metodyki zarządzania ryzykiem cyberprzestrzeni w jednostkach sektora publicznego w rozumieniu pkt 3.1. *Polityki* oraz przygotowanie wzoru sprawozdania z szacowania ryzyka. Termin realizacji zamówienia wyznaczono na dzień 10 lutego 2014 r., a wydatki na realizację umowy wyniosły 3,7 tys. zł.

(dowód: akta kontroli tom IV str. 18-76, 114-115)

W dniu 31 stycznia 2014 r. do MAiC wpłynęła, opracowana przez Zespół CERT.GOV.PL. działający w ramach ABW, metodyka szacowania ryzyka cyberprzestrzeni, zawierająca m.in. katalog przykładowych zagrożeń i wzór sprawozdania z analizy ryzyka. Przedmiotowa metodyka została otrzymana w dniu 31 stycznia 2014 r. przez Podsekretarza Stanu w MAiC – Pana Romana

³⁴ Aktualizacja została dokonana na wniosek RCB, w ramach wymaganej przepisami, dokonywanej nie rzadziej, niż co dwa lata, aktualizacji Raportu o zagrożeniach bezpieczeństwa narodowego.

Dmowskiego, a następnie w dniu 14 lutego 2014 r., przekazana do właściwej komórki merytorycznej, tj. do DSI.

(dowód: akta kontroli tom IV str. 1-17)

Podsekretarz Stanu w MAiC – Pan Roman Dmowski zeznał, iż przyczyną opóźnienia w rozpoczęciu przygotowania szacowania ryzyka IT za rok 2013 w stosunku do terminu wynikającego z *Polityki* był fakt, iż w drugiej połowie 2013 r. w Ministerstwie nie było jeszcze wyznaczonej komórki organizacyjnej odpowiadającej za realizację tych zadań.

(dowód: akta kontroli tom III str. 466-474)

Na etapie prac nad metodyką szacowania ryzyka, MAiC nie prowadziło konsultacji z innymi administratorami i użytkownikami cyberprzestrzeni dotyczących treści tego dokumentu, co wyjaśniano brakiem takiego wymogu, zaufaniem do Wykonawcy oraz brakiem czasu. W szczególności nie podjęto współpracy z RCB w celu zapewnienia porównywalności i komplementarności metod szacowania ryzyka wykorzystywanych przez te podmioty oraz wyników identyfikacji kluczowych, krajowych zasobów teleinformatycznych przeprowadzanej przez MAiC i przez RCB. Podsekretarz Stanu w MAiC – Pan Roman Dmowski wyjaśnił, m.in. że: (...) *Żaden przepis Polityki nie nakazuje (...) stosowania tych samych norm, metodyk czy procedur. (...) W szczególności należy podkreślić, że ani w pkt. 2, ani w pkt. 3.1, poświęconym szacowaniu ryzyka, Polityka nie nakazuje ani wprost, ani w sposób dorozumiany, aby metodyka szacowania ryzyka była tożsama lub dostosowana do metodyki stosowanej w ramach procesów szacowania ryzyka infrastruktury krytycznej. (...) Powyższe nie oznacza oczywiście, że zbliżanie metod szacowania w obu procesach nie byłoby korzystne i że DSI nie zamierza podjąć działań zmierzających do zapewnienia możliwie ścisłej ich porównywalności. (...).*

MAiC nie prowadziło również współpracy z ABW oraz z Zespołem CERT.GOV.PL. w celu określenia założeń metodyki szacowania ryzyka. Zarówno pracownicy DSI, realizujący od stycznia 2014 r. obowiązki związane z ochroną cyberprzestrzeni, jak i Podsekretarz Stanu odpowiadający za te zadania od września 2013 r. nie dysponowali wiedzą na temat prac prowadzonych przez ABW nad projektem metodyki. Pracownicy DSI wyjaśnili: *zadania związane z ochroną cyberprzestrzeni zostały przekazane do Wydziału Unii Europejskiej i Spraw Międzynarodowych w styczniu br. Nie było żadnej ciągłości instytucjonalnej i Wydział nie dysponował wiedzą na temat prac prowadzonych nad metodyką przez ABW. Dlatego też DSI nie prowadziło żadnej współpracy z ABW w ww. zakresie.*

Podsekretarz Stanu w MAiC – Pan Roman Dmowski zeznał: *W momencie podejmowania decyzji nie miałem informacji, że metodyka ABW jest gotowa. Nie mieliśmy również informacji, kiedy ten dokument będzie gotowy i dopiero w momencie, gdy wyraziłem zgodę na zamówienie gotowej metodyki wpłynął dokument z ABW. Ponieważ zależało nam na uruchomieniu procesu szacowania ryzyka, zdecydowaliśmy się na szybki zakup gotowej metodyki (...).*

(dowód: akta kontroli tom III str. 466-474, tom IV str. 1-76, 114-115, tom V str. 1-10, 83-119)

W trakcie kontroli NIK, zostały rozpoczęte konsultacje Kierownictwa MAiC i RCB, w wyniku których uzgodniono m.in., iż zostaną podjęte starania, aby osiągnąć komplementarność metod oceny ryzyka wykorzystywanych przez obie instytucje.

(dowód: akta kontroli tom V str. 121-122)

Zakupiona metodyka oraz wzór sprawozdania z analizy ryzyka zostały przekazane, w dniu 13 lutego 2014 r., do 95 instytucji państwowych z prośbą o oszacowanie ryzyka i przekazanie do MAiC wypełnionych sprawozdań w terminie do dnia

31 marca 2014 r. W Ministerstwie nie został natomiast opracowany kompleksowy wykaz podmiotów administracji rządowej zobowiązanych do stosowania *Polityki*. W szczególności, DSI nie dysponował pełnym wykazem dotyczącym liczby oraz rodzaju urzędów administracji zespolonej i niezespolonej, w których powinna być wdrażana *Polityka*, w związku z czym nie było możliwości określenia precyzyjnej liczby podmiotów zobowiązanych do oszacowania ryzyka.

Podsekretarz Stanu w MAiC – Pan Roman Dmowski wyjaśnił, że szacowanie ryzyka za 2013 r. zostało zrealizowane we wstępnej formule i jednym z jego celów było doprecyzowanie pożądanej formuły obowiązków sprawozdawczych na lata kolejne.
(dowód: akta kontroli tom III str. 334-345, tom IV str. 18-113, 134-169, 238-240, 256-278)

Zgodnie z zakupioną przez MAiC metodyką, kluczowym etapem analizy ryzyka było zidentyfikowanie przez jednostki krytycznych zasobów teleinformatycznych. W ww. dokumencie nie określono natomiast precyzyjnych (porównywalnych) kryteriów identyfikacji zasobów krytycznych.

Naczelnik Wydziału Unii Europejskiej i Spraw Międzynarodowych DSI wyjaśnił, że *na chwilę obecną nie ma możliwości oceny poprawności rozwiązania zastosowanego w metodyce w zakresie identyfikacji krytycznych zasobów teleinformatycznych. Zasadność przyjętego podejścia zostanie zweryfikowana w wyniku analizy wyników przeprowadzonego szacowania ryzyka.*

Podsekretarz Stanu w MAiC – Pan Roman Dmowski zeznał: *Nie mam takiej wiedzy, żeby porównywać, czy metodyka jest prawidłowa, czy nie. Nie widziałam metodyki na 2014 r. Nowo zatrudniony pracownik DSI ma doświadczenie z zakresu bezpieczeństwa systemów i weryfikował ten dokument. Nie jestem kompetentny, żeby dokonywać oceny tego dokumentu.*

(dowód: akta kontroli tom III str. 466-474, tom IV str. 23-40, 72-76)

W wyniku analizy dokumentacji z szacowania ryzyka ustalono, że część podmiotów administracji rządowej nie wywiązała się z obowiązku określonego w pkt 3.1. *Polityki*, tj. nie przekazała do MAiC sprawozdań z analizy ryzyka (np. Minister Spraw Wewnętrznych, Minister Spraw Zagranicznych, Minister Sprawiedliwości, Minister Zdrowia, Prezes Urzędu Lotnictwa Cywilnego). W przypadku niektórych podmiotów sprawozdania były niekompletne, zawierały błędy, zostały sporządzone w oparciu o inną metodykę lub na niewłaściwym formularzu. MAiC nie występowało z monitami do podmiotów, które nie zrealizowały obowiązków z zakresu szacowania ryzyka lub przesyłały niekompletne (błędnie przygotowane) sprawozdania.

Pracownicy DSI wyjaśnili, że: (...) *szacowanie ryzyka za 2013 r. ma pilotażowy charakter. Ponadto merytoryczna analiza wszystkich otrzymanych sprawozdań nastręcza problemów, ze względu na ograniczone możliwości kadrowe Wydziału. Nie podejmowano więc działań w celu zwiększenia liczby otrzymanych sprawozdań.*

(dowód: akta kontroli tom IV str. 72-133, 252-278)

Do końca okresu objętego kontrolą, w MAiC nie opracowano ostatecznego sprawozdania z szacowania ryzyka związanego z funkcjonowaniem cyberprzestrzeni, ani metodyki analizy ryzyka za 2014 r. Kontrolującemu przedstawiono projekt sprawozdania za 2013 rok z dnia 2 grudnia 2014 r., zatwierdzony przez Naczelnika Wydziału Unii Europejskiej i Spraw Międzynarodowych DSI. Projekt metodyki szacowania ryzyka za 2014 r. został przekazany, w dniu 17 listopada 2014 r., podmiotom uczestniczącym w pracach *Zespołu zadaniowego do spraw bezpieczeństwa cyberprzestrzeni Rzeczypospolitej Polskiej* i miał być przedmiotem obrad drugiego posiedzenia tego Zespołu.

(dowód: akta kontroli tom III str. 339-353, tom IV str. 256-278, 455-457)

Audyt wewnętrzny zlecony w zakresie bezpieczeństwa teleinformatycznego podmiotów administracji państwowej.

W okresie wrzesień – październik 2013 r. na polecenie Prezesa Rady Ministrów, w 314 jednostkach administracji państwowej, został przeprowadzony zlecony audyt wewnętrzny dotyczący bezpieczeństwa teleinformatycznego. Założenia merytoryczne i organizacyjne audytu zostały wypracowane m.in. przez Zespół zadaniowy do spraw ochrony portali rządowych, przy udziale pracowników Gabinetu Politycznego Ministra Administracji i Cyfryzacji. Dokumentacja źródłowa z audytu została zgromadzona w Ministerstwie Finansów, a następnie w listopadzie 2013 r., przekazana Ministrowi Administracji i Cyfryzacji, który odpowiadał za sporządzenie zbiorczego sprawozdania audytowego.

Wg stanu na dzień zakończenia kontroli, nie zostało sporządzone i przekazane podmiotom realizującym zadania związane z ochroną cyberprzestrzeni RP, w tym w szczególności Prezesowi Rady Ministrów, zbiorcze sprawozdanie, obejmujące m.in. wnioski i rekomendacje z realizacji w ww. audytu zleconego. W MAiC opracowano, w oparciu o elektroniczne dane zagregowane przez MF, wstępne, sumaryczne zestawienie, wybranych przez Podsekretarza Stanu w MAiC – Pana Romana Dmowskiego, odpowiedzi z poszczególnych ankiet audytowych. Nie przeprowadzono przy tym żadnej analizy dokumentacji źródłowej z audytu wewnętrznego przekazanej do MAiC – obejmującej 19 kartonów: ankiet, arkuszy z wyjaśnieniami oraz opinii, wniosków i rekomendacji przygotowanych przez audytorów z poszczególnych jednostek. Wstępne zestawienie danych z przeprowadzonego audytu zostało przedstawione podczas pierwszego posiedzenia Zespołu zadaniowego do spraw bezpieczeństwa cyberprzestrzeni Rzeczypospolitej Polskiej, w dniu 28 lipca 2014 r.

(dowód: akta kontroli tom III str. 1-345, tom IV str. 367-369)

Naczelnik Wydziału Unii Europejskiej i Spraw Międzynarodowych DSI wyjaśnił, że: *nie zostały dotychczas opracowane wnioski i rekomendacje z raportu, ponieważ od początku przyjęto założenie, że analiza wyników audytu będzie przedmiotem prac nowo powołanego zespołu ds. bezpieczeństwa cyberprzestrzeni. Nie przewidywaliśmy, że wystąpi tak znaczne opóźnienie w powołaniu tego zespołu. Ponadto należy zaznaczyć, że ze względu na ograniczone możliwości kadrowe i ograniczenia wiedzy technicznej pracowników DSI, wypracowanie takich rekomendacji byłoby utrudnione.*

(dowód: akta kontroli tom III str. 53-55)

Podsekretarz Stanu w MAiC – Pana Roman Dmowski zeznał: *W mojej ocenie częściowe sprawozdanie zawiera wszystkie najważniejsze informacje wynikające z tego audytu. Celem tego audytu było pozyskanie informacji o poziomie zabezpieczeń w jednostkach administracji publicznej, na podstawie których będzie można podejmować decyzje określające priorytetowe kierunki działań i te informacje są wykorzystywane w pracach nad Planem działań tworzoną przez Zespół. Część informacji szczegółowych, które nie zostały wykorzystane w sprawozdaniu będzie wykorzystana w kolejnych latach jako wyznacznik zmian następujących w obszarze bezpieczeństwa cyberprzestrzeni. (...) Być może ostateczna forma sprawozdania będzie podlegała jeszcze modyfikacjom. Na tym etapie zestawienie danych było przygotowane dla Członków Zespołu międzyresortowego, tj. osób fachowo zaangażowanych w tematykę bezpieczeństwa IT.(...) To Zespół odpowiada za wypracowanie kierunków działań wynikających z tego dokumentu. Zostaną one zawarte w Planie działań.*

(dowód: akta kontroli tom III str. 466-474)

Na zadane w tej sprawie Prezesowi Rady Ministrów pytanie odpowiedział Szef Kancelarii Prezesa Rady Ministrów – Pan Jacek Cichocki, który wyjaśnił, iż nie podejmowano działań w celu zobligowania Ministra Administracji i Cyfryzacji do sporządzenia i przekazania Prezesowi Rady Ministrów zbiorczego sprawozdania z wyników ww. zleconego audytu wewnętrznego, ponieważ to Minister Administracji i Cyfryzacji odpowiada za realizację tych zadań. Wskazał również, że koordynacja audytu wewnętrznego należy do Ministra Finansów.

(dowód: akta kontroli tom III str. 481-484)

Ustalone
nieprawidłowości

1. Kontrola wykazała, że opracowany w MAiC w 2012 r. raport cząstkowy Ministra Administracji i Cyfryzacji o zagrożeniach bezpieczeństwa narodowego został przygotowany w sposób nierzetelny. W przedmiotowym dokumencie w sposób zawężony i nieodpowiadający stanowi faktycznemu opisano zagrożenia związane z cyberprzestrzenią oraz zadania Ministra Administracji i Cyfryzacji w zakresie zarządzania tymi zdarzeniami. Przez okres ponad roku od wejścia w życie *Polityki*, nie podjęto również żadnych działań w celu dokonania aktualizacji tego dokumentu. Przyczynami ww. nieprawidłowości był brak kompleksowego zdefiniowania zadań Ministra Administracji i Cyfryzacji związanych z bezpieczeństwem teleinformatycznym państwa oraz nieprzypisanie adekwatnych zasobów do ich realizacji. Nierzetelne przygotowanie raportu cząstkowego o zagrożeniach bezpieczeństwa narodowego wpłynęło również na treść opracowanego na jego podstawie Krajowego Planu Zarządzania Kryzysowego (opisano szczegółowo na str. 31 wystąpienia pokontrolnego).
2. W ocenie NIK, Minister Administracji i Cyfryzacji w sposób nierzetelny przygotował i koordynował realizację zadania wymienionego w pkt 3.1. *Polityki*, dotyczącego oszacowania ryzyk związanych ze zdarzeniami występującymi w cyberprzestrzeni RP, i tak:
 - w MAiC z opóźnieniem przystąpiono do przygotowania procesu szacowania ryzyka cyberprzestrzeni za 2013 r. Przez okres ponad pół roku od wejścia w życie *Polityki* nie podjęto żadnych działań w tym zakresie, a czynności mające na celu wytworzenie metodyki analizy ryzyka zostały podjęte dopiero pod koniec stycznia 2014 r., tj. w momencie, w którym proces szacowania powinien być już zakończony. W związku z powyższym, analiza ryzyka za 2013 r. nie została przygotowana z należytą starannością. Nie przeprowadzono konsultacji z innymi podmiotami realizującymi zadania z zakresu szacowania ryzyka dla krytycznej infrastruktury państwa (w szczególności z RCB) oraz nie współpracowano z ABW i nie dysponowano wiedzą o prowadzonych w tej instytucji pracach nad metodyką szacowania ryzyka. W rezultacie, zakupiono w pośpiechu, wytworzoną w ciągu 4 dni metodykę, a Kierownictwo Ministerstwa i pracownicy odpowiadający za szacowanie ryzyka nie byli w stanie ocenić merytorycznej jakości tego dokumentu. W MAiC nie opracowano pełnego wykazu instytucji zobowiązanych do wdrażania *Polityki*, w związku z czym nie dysponowano precyzyjną wiedzą na temat liczby i rodzaju podmiotów administracji rządowej, które były zobowiązane do wykonania analizy ryzyka. Należy również podkreślić, że Kierownictwo Ministerstwa nie przypisało zasobów adekwatnych do realizacji zadań związanych z przygotowaniem procesu szacowania ryzyka oraz z analizą przekazywanych do MAiC wyników tego szacowania;
 - brak rzetelnego przygotowania wpłynął negatywnie na jakość wyników szacowania ryzyka za 2013 r., które powinny były określić podstawowe kierunki działań w zakresie ochrony cyberprzestrzeni RP. Stwierdzono, że ze względu na niewystarczające zasoby kadrowe nie występowało do podmiotów, które nie przygotowały sprawozdań z analizy ryzyka, lub przygotowały je w sposób

nieprawidłowy, co skutkowało niekompletnością i brakiem porównywalności wyników szacowania ryzyka. Do końca kontroli nie zostało również opracowane ostateczne sprawozdanie z analizy ryzyka za 2013 r. oraz metodyka szacowania ryzyka za 2014 r., co m.in. może skutkować opóźnieniem w realizacji tych zadań w roku kolejnym.

3. Ustalono, że do dnia rozpoczęcia kontroli, w MAiC nie został zrealizowany obowiązek określony w pkt 3.1. *Polityki*, dotyczący oszacowania ryzyka dla systemów teleinformatycznych wykorzystywanych do realizacji zadań Ministra Administracji i Cyfryzacji. Sprawozdanie z analizy ryzyka dla MAiC zostało sporządzone dopiero po otrzymaniu pisma kontrolującego w ww. sprawie, a ponadto nie było ono w pełni zgodne z metodyką i wzorem przekazanymi przez MAiC innym podmiotom. Minister Administracji i Cyfryzacji wyjaśnił, że opóźnienie w przygotowaniu sprawozdania z szacowania ryzyka dla własnych systemów teleinformatycznych wynikało z konieczności zespolenia wkładów przygotowanych przez różne komórki organizacyjne Ministerstwa.

(dowód: akta kontroli tom I str. 383-396, tom IV str. 133, 177- 237, tom V str. 83-105)

4. NIK ocenia jako nierzetelne, brak opracowania i wykorzystania w ramach realizacji zadań związanych z ochroną cyberprzestrzeni, kompleksowego sprawozdania z przeprowadzonego w 2013 r. audytu zleconego w zakresie bezpieczeństwa teleinformatycznego podmiotów państwowych. W ocenie NIK, po upływie roku, znaczna część ustaleń ww. audytu uległa dezaktualizacji, co ogranicza możliwość dalszego wykorzystania uzyskanych w jego wyniku informacji.

Odpowiedzialność za opisane powyżej nieprawidłowości ponoszą osoby zajmujące w latach 2011 – 2014 stanowisko Ministra Administracji i Cyfryzacji oraz Pan Roman Dmowski – Podsekretarz Stanu w MAiC, któremu od września 2013 r. powierzono zadania związane z ochroną cyberprzestrzeni RP.

Uwagi dotyczące
badanej działalności

NIK zwraca uwagę, iż brak systemowego planowania, skutkuje niegospodarnym wykorzystaniem ograniczonych zasobów przeznaczonych na realizację zadań w zakresie ochrony cyberprzestrzeni RP. Stwierdzono bowiem, że w wyniku zastosowania zakupionej przez MAiC metodyki szacowania ryzyka, w Ministerstwie tworzona jest obecnie ewidencja krytycznych zasobów teleinformatycznych administracji rządowej, podczas gdy wykaz infrastruktury krytycznej, zawierający m.in. takie systemy, prowadzony jest przez RCB. Przykładem niegospodarnego zarządzania zasobami jest także opisany powyżej brak kompleksowego wykorzystania ustaleń audytu wewnętrznego, w którego realizację zaangażowano audytorów wewnętrznych z 314 instytucji państwowych oraz pracowników MF i MAiC.

Ocena częściowa

Najwyższa Izba Kontroli ocenia negatywnie dotychczasową działalność Ministra Administracji i Cyfryzacji w zakresie szacowania ryzyk związanych ze zdarzeniami występującymi w cyberprzestrzeni.

3. Realizacja zadań związanych z ochroną cyberprzestrzeni.

Koordinacja krajowego systemu reagowania na incydenty w cyberprzestrzeni.

Na podstawie pkt 4.2. *Polityki* ustanowiony został trzypoziomowy Krajowy System Reagowania na Incydenty Komputerowe w Cyberprzestrzeni RP obejmujący:

- Poziom I – poziom koordynacji – minister właściwy ds. informatyzacji;

- Poziom II – poziom reagowania na incydenty komputerowe – Zespół CERT.GOV.PL w sferze cywilnej oraz Zespół CERT-MIL³⁵ w sferze militarnej;
- Poziom III – poziom realizacji – administratorzy odpowiadający za poszczególne systemy teleinformatyczne funkcjonujące w cyberprzestrzeni.

Ustalano, że Minister Administracji i Cyfryzacji nie podjął działań mających na celu wdrożenie zapisów *Polityki* dotyczących funkcjonowania krajowego systemu reagowania na incydenty komputerowe w cyberprzestrzeni RP. Wg stanu na dzień zakończenia kontroli, nie został zorganizowany system wymiany informacji między MAiC a Zespołami CERT oraz innymi użytkownikami i administratorami cyberprzestrzeni. W Ministerstwie nie pozyskiwano i nie ewidencjonowano informacji na temat incydentów komputerowych występujących w cyberprzestrzeni oraz nie realizowano i nie inicjowano działań wymienionych w pkt 3.6.2. oraz 3.6.5. *Polityki*, dotyczących rozbudowy zespołów reagowania na incydenty komputerowe. Minister Administracji i Cyfryzacji nie podejmował działań w celu ustanowienia w Polsce narodowego Zespołu CERT, ani nie dysponował wiedzą o strukturze, zasobach oraz o usługach świadczonych przez funkcjonujące państwowe zespoły CERT. W MAiC nie przeprowadzano żadnych analiz pozwalających na oszacowania niezbędnych zasobów państwowych zespołów CERT.

Podsekretarz Stanu w MAiC – Pan Roman Dmowski wyjaśnił, m.in. że Ministerstwo nie ma narzędzi prawnych, ani wystarczających zasobów (w szczególności kadrowych) do realizacji ww. zadań koordynatora krajowego systemu reagowania na incydenty komputerowe w cyberprzestrzeni RP. Wskazał, że Minister Administracji i Cyfryzacji nie nadzoruje państwowych Zespołów CERT i ma utrudniony dostęp do Zespołu CERT.GOV.PL. Wyjaśnił także: (...) *Pamiętać należy jednak, że Polityka jako rządowy dokument programowy, nie posiada waloru wiążącego aktu prawnego.*

Odnosnie braku działań w celu powołania CERTu narodowego, Podsekretarz Stanu w MAiC – Pan Roman Dmowski zeznał: *W celu przeprowadzenia takich działań potrzebna jest definicja CERTU narodowego. Nasze działania koncentrują się na dyrektywie NIS, która określi, jakie wymagania musi spełniać Zespół CERT, aby można go było określić CERTEM narodowym.*

(dowód: akta kontroli tom I str. 153-183, tom III str. 466-474)

Z wyjaśnień Kierownictwa MAiC wynika, że w ramach koordynacji krajowego systemu reagowania na incydenty komputerowe w cyberprzestrzeni RP zorganizowano 2 spotkania z przedstawicielami administracji rządowej dotyczące m.in. prac nad dyrektywą NIS oraz podejmowano działania dotyczące popularyzacji idei ustanowienia pełnomocników do spraw bezpieczeństwa cyberprzestrzeni.

(dowód: akta kontroli tom I str. 163, tom III str. 415)

W DSI MAiC została opracowana i była na bieżąco aktualizowana baza danych³⁶ zawierająca imiona i nazwiska oraz dane kontaktowe pełnomocników ds. bezpieczeństwa cyberprzestrzeni wyznaczonych przez poszczególne instytucje państwowe. W MAiC nie został zorganizowany system szkoleń pełnomocników ds. bezpieczeństwa cyberprzestrzeni, natomiast w drugiej połowie 2014 r. zorganizowano dwa szkolenia skierowane do osób zajmujących to stanowisko.

(dowód: akta kontroli tom I str. 153-183, 266, tom III str. 377-382, tom IV str. 106-113, 241-250, 279-295)

³⁵ Zespół CERT-MIL jest zespołem reagowania na incydenty komputerowe funkcjonującym w resorcie obrony narodowej.

³⁶ Wg stanu na dzień 18 listopada 2014 r. baza danych zawierała dane kontaktowe 99 pełnomocników.

Ustanowienie i kontrola wymogów w zakresie bezpieczeństwa cyberprzestrzeni.

W wyniku prac *Zespołu zadaniowego do spraw ochrony portali rządowych* zostały przygotowane następujące wytyczne dotyczące bezpieczeństwa IT:

- Wytyczne Ministra Administracji i Cyfryzacji w zakresie ochrony portali informacyjnych administracji publicznej z dnia 26 stycznia 2012 r.;
- Wytyczne bezpieczeństwa dla administracji (wydane przez ABW).

Monitoring stanu wdrożenia ww. wytycznych był prowadzony w 2013 r. przez ABW przy udziale pracowników Gabinetu Politycznego Ministra Administracji i Cyfryzacji. Od momentu przekazania zadań związanych z ochroną cyberprzestrzeni do DSI, MAiC nie weryfikowało i nie monitorowało przestrzegania przedmiotowych wytycznych. Podsekretarz Stanu w MAiC – Pan Roman Dmowski wyjaśnił, że brak działań w tym zakresie wynikał z ograniczonej liczby pracowników DSI.

(dowód: akta kontroli tom I str. 153-202, 233-236, 294-366)

W MAiC nie podjęto działań w celu przygotowania projektów:

- propozycji działań dla jednostek administracji rządowej, mających na celu ochronę systemów teleinformatycznych przed cyberatakami,
- standardów bezpieczeństwa dla systemów teleinformatycznych jednostek administracji rządowej i usług funkcjonujących w ramach tych systemów,

pomimo iż ww. wytyczne, powinny być zostać przygotowane przez *Zespół zadaniowy do spraw bezpieczeństwa cyberprzestrzeni Rzeczypospolitej Polskiej* w terminie do dnia 13 grudnia 2014 r.

Podsekretarz Stanu w MAiC – Pan Roman Dmowski wyjaśnił, że prace nad ww. dokumentami nie zostały jeszcze podjęte, ponieważ jako priorytetowe zadanie uznano przygotowanie *Planu działań w zakresie zapewnienia bezpieczeństwa cyberprzestrzeni RP*.

(dowód: akta kontroli tom I str. 174)

W całym okresie objętym kontrolą, Minister Administracji i Cyfryzacji nie realizował, w stosunku do podmiotów podległych lub nadzorowanych oraz innych podmiotów publicznych, obowiązków kontrolnych wymienionych w art. 25 ust. 1 pkt 3 lit. b) i c) ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne (zwanej dalej ustawą o informatyzacji), w tym w zakresie sprawdzenia zabezpieczeń systemów teleinformatycznych wykorzystywanych przez te jednostki³⁷. Minister nie kierował wytycznych do wojewodów dotyczących sposobu realizacji nałożonych na nich, na podstawie art. 25 powołanej ustawy, obowiązków kontroli systemów teleinformatycznych jednostek samorządu terytorialnego. Nie występowano również do Ministra Finansów o przydzielenie dodatkowych środków finansowych na realizację zadań przewidzianych w ww. przepisach.

Z wyjaśnień Kierownictwa MAiC wynika, że nie realizowano obowiązków określonych w art. 25 ustawy o informatyzacji, ponieważ od momentu nowelizacji ww. ustawy w 2010 r., która zniósła obowiązek rejestrowania systemów teleinformatycznych, nie dysponowano wiedzą na temat katalogu systemów wykorzystywanych do realizacji zadań publicznych. Wyjaśniono także, że przedmiotowe kontrole nie były zgłaszane do planu kontroli przez Członków Kierownictwa MAiC, ani przez komórki organizacyjne Ministerstwa, a pracownicy

³⁷ Obowiązek wdrożenia i doskonalenia systemów zarządzania bezpieczeństwem informacji wynika z § 20 rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz. U. z 2012 r., poz. 526 ze zm.)

Departamentu Kontroli, Skarg i Wniosków MAiC nie posiadali certyfikatów uprawniających do prowadzenia kontroli systemów teleinformatycznych. Minister Administracji i Cyfryzacji wskazał, że inwentaryzacja systemów wykorzystywanych do realizacji zadań publicznych planowana jest w ramach Programu Zintegrowanej Informatyzacji Państwa, który został przyjęty przez Radę Ministrów w styczniu 2014 r. Poinformował również, że MAiC występowało z inicjatywą legislacyjną dotyczącą uchylecia rozdziału 4 ustawy o informatyzacji, w którym określono obowiązki w zakresie kontroli przestrzegania przepisów tej ustawy.

(dowód: akta kontroli tom V str. 424-514)

Minister Administracji i Cyfryzacji wyjaśnił, że nie wykorzystywano mechanizmów kontrolnych ustanowionych na podstawie art. 25 ustawy o informatyzacji w ramach realizacji zadań związanych z ochroną cyberprzestrzeni, ponieważ *Polityka* jest dokumentem o charakterze strategiczno-programowym i nie formułuje wprost obowiązków kontrolnych dla Ministra, które są charakterystyczne dla rozwiązań ustawowych. (...) *A zatem w świetle wymienionych zapisów nie było uzasadnienia do wykorzystania mechanizmów kontrolnych ustanowionych na podstawie (...) ustawy o informatyzacji (...) w ramach koordynacji wdrażania Polityki ochrony cyberprzestrzeni RP. Mechanizm ten został uchwalony i powinien funkcjonować niezależnie od Polityki, a jego kontrola powinna być elementem kontroli zarządczej w jednostkach administracji rządowej.*

(dowód: akta kontroli tom V str. 489-490)

W związku z przeprowadzoną przez NIK, w okresie maj - lipiec 2014 r., w MAiC kontrolą dotyczącą krajowych ram interoperacyjności³⁸, zostały podjęte działania mające na celu zapewnienie warunków realizacji obowiązków Ministra Administracji i Cyfryzacji, wynikających z art. 25 ustawy o informatyzacji. Skierowano 2 pracowników Departamentu Kontroli, Skarg i Wniosków na szkolenia specjalistyczne uprawniające do kontroli systemów teleinformatycznych oraz wszczęto procedurę naboru dodatkowego pracownika z wymaganymi uprawnieniami.

(dowód: akta kontroli V str. 479-490)

Rozwój narodowych planów kryzysowych.

Z wyjaśnień Kierownictwa MAiC wynika, że w Polsce, w związku z zagrożeniami dla krytycznych systemów teleinformatycznych tworzone są następujące plany kryzysowe:

- plany zarządzania kryzysowego, sporządzane na podstawie ustawy o zarządzaniu kryzysowym;
- plany ochrony infrastruktury krytycznej, sporządzane na podstawie ww. ustawy przez operatorów obiektów wymienionych w wykazie infrastruktury krytycznej;
- plany działań w sytuacjach szczególnych zagrożeń, sporządzane przez przedsiębiorców telekomunikacyjnych, na podstawie Prawa telekomunikacyjnego.

Dyrektor DSI wyjaśnił, że podległy mu Departament nie jest komórką organizacyjną MAiC właściwą do udzielania wyjaśnień na temat planów kryzysowych związanych z zagrożeniami dla krytycznych systemów teleinformatycznych.

(dowód: akta kontroli tom V str. 83-119)

Minister Administracji i Cyfryzacji nie kierował do RCB wytycznych, zaleceń, itp. w zakresie sposobu identyfikacji oraz zarządzania ryzykami dotyczącymi kluczowych, państwowych systemów teleinformatycznych, które powinny być

³⁸ Kontrola nr P/14/004 pt. *Wdrażanie wybranych wymagań dotyczących systemów teleinformatycznych, wymiany informacji w postaci elektronicznej oraz Krajowych Ram Interoperacyjności na przykładzie niektórych urzędów gmin miejskich i miast na prawach powiatu.*

wykorzystane w ramach realizacji zadań tego podmiotu wynikających z ustawy o zarządzaniu kryzysowym.

Podsekretarz Stanu w MAiC – Pan Roman Dmowski wyjaśnił, że nie stwierdzono dotychczas konieczności wydawania takich wytycznych, a ponadto żaden dokument nie nakłada na Ministra takiego obowiązku.

(dowód: akta kontroli tom V str. 96-105)

W Krajowym Planie Zarządzania Kryzysowego³⁹ (zwanym dalej KPZK) zawarto ogólną definicję zagrożeń występujących w cyberprzestrzeni, natomiast nie wykazano zdarzeń kryzysowych związanych z cyberprzestrzenią w siatce bezpieczeństwa określającej zadania i obowiązki uczestników zarządzania kryzysowego w podziale na poszczególne fazy zarządzania kryzysowego⁴⁰. W związku z powyższym, w ww. dokumencie w ogóle nie zawarto zadań i podmiotów odpowiedzialnych za zarządzanie zdarzeniami kryzysowymi występującymi w cyberprzestrzeni oraz pominięto wiodącą rolę Ministra Administracji i Cyfryzacji w zarządzaniu tymi zagrożeniami. Propozycja uzupełniania KPZK o zagrożenia w cyberprzestrzeni została zgłoszona na etapie uzgodnień międzyresortowych przez Biuro Bezpieczeństwa Narodowego, natomiast zgodnie ze stanowiskiem MAiC, uzupełnienie Planu o podmioty wiodące i współpracujące oraz konkretne zadania w przypadku zagrożeń cyberprzestrzeni miało zostać dokonane po przyjęciu *Polityki*.

Do dnia rozpoczęcia kontroli NIK, Minister Administracji i Cyfryzacji nie podejmował działań mających na celu aktualizację KPZK, poprzez wskazanie w tym dokumencie zadań i podmiotów odpowiedzialnych za zarządzanie zdarzeniami kryzysowymi występującymi w cyberprzestrzeni oraz wiodącej roli MAiC w tym zakresie. Podsekretarz Stanu w MAiC – Pan Roman Dmowski wyjaśnił, że nie występowało z wnioskiem o aktualizację KPZK, ponieważ nie otrzymano sygnałów od innych instytucji (w tym od RCB) o takiej potrzebie. Wskazał również, że ograniczone zasoby kadrowe MAiC uniemożliwiły analizę tego dokumentu.

(dowód: akta kontroli tom V str. 1-17, 83-119)

W trakcie kontroli NIK, z inicjatywy RCB, została rozpoczęta aktualizacja KPZK, w ramach której przygotowano m.in. siatkę bezpieczeństwa dotyczącą zagrożeń w cyberprzestrzeni. W projekcie ww. dokumentu, dla żadnej z faz zarządzania kryzysowego, MAiC nie zostało wskazane jako podmiot wiodący, a tylko jako podmiot wspomagający zadania (podmiotem wiodącym dla każdej z faz była ABW). Projekt ww. dokumentu był opiniowany przez MAiC, natomiast Minister Administracji i Cyfryzacji nie wniósł uwag odnoszących się do wiodącej roli Ministerstwa w zakresie zarządzania zdarzeniami związanymi z cyberprzestrzenią.

Dyrektor DSI wyjaśnił: *W mojej opinii obecnie ABW jest przygotowana do pełnienia tej funkcji dużo lepiej niż MAiC, posiada odpowiednią infrastrukturę i zasoby kadrowe. Departament Społeczeństwa Informacyjnego nie jest w stanie pełnić tej funkcji lepiej od ABW, ponieważ nie posiada tak dobrych kadr i zasobów. W mojej ocenie, przypisanie takiej funkcji ABW nie jest sprzeczne z Polityką.*

(dowód: akta kontroli tom V str. 1-10, 124)

Od momentu utworzenia Ministerstwa do dnia zakończenia kontroli, nie został opracowany i uzgodniony z Dyrektorem RCB Plan Zarządzania Kryzysowego (PKZ) MAiC. W projekcie ww. dokumentu⁴¹ wymieniono zagrożenia występujące w cyberprzestrzeni oraz zawarto krótki opis systemu monitorowania tych zagrożeń.

³⁹ Wersja znowelizowana na podstawie uchwały Rady Ministrów z dnia 23 lipca 2013 r.

⁴⁰ Zapobieganie, przygotowanie, reagowanie, odbudowa.

⁴¹ Wersja z dnia 24 lutego 2014 r. przekazana do RCB.

W projekcie PZK MAiC nie wskazano natomiast dla zagrożeń występujących w cyberprzestrzeni, zagadnień wymienionych w art. 12 ust. 2 pkt 2 ustawy o zarządzaniu kryzysowym, tj. szczegółowych sposobów i środków reagowania na zagrożenia oraz ograniczania i likwidacji ich skutków. Nie uwzględniono również wiodącej roli Ministra Administracji i Cyfryzacji w zarządzaniu zagrożeniami występujących w cyberprzestrzeni RP. Ponadto, w siatce bezpieczeństwa, nie wskazano DSI, który od stycznia 2014 r. jest komórką organizacyjną MAiC wiodącą w obszarze ochrony cyberprzestrzeni. Na etapie wewnątrzresortowych uzgodnień projektu PZK MAiC, prowadzonych w lutym 2014 r., zarówno Członek Kierownictwa Ministerstwa odpowiadający za ochronę cyberprzestrzeni, jak i Kierownictwo DSI nie zgłosili żadnych uwag dotyczących treści projektu PZK MAiC w tym zakresie.

Dyrektor DSI wyjaśnił: *W tym okresie tematyka ochrony cyberprzestrzeni oraz jej powiązanie z systemem zarządzania kryzysowego były nowym zagadnieniem, dopiero przekazany do DSI, co nie pozwoliło na sformułowanie precyzyjnych, merytorycznych uwag w tym zakresie. Ponadto obłożenie innymi obowiązkami powodowało, że nie było możliwości poświęcenia wystarczającej ilości czasu na przygotowanie kompetentnej odpowiedzi.*

(dowód: akta kontroli tom V str. 1-10, 18-82, 120)

Wg stanu na dzień 28 listopada 2014 r., w MAiC były prowadzone prace nad nową wersją Planu Zarządzania Kryzysowego Ministerstwa, mające m.in. na celu ujęcie w tym dokumencie zagrożeń i zadań związanych z cyberprzestrzenią.

(dowód: akta kontroli tom V str. 123)

Organizacja ćwiczeń i testów systemu bezpieczeństwa cyberprzestrzeni RP.

W okresie objętym kontrolą, Minister Administracji i Cyfryzacji nie był organizatorem ćwiczeń systemu bezpieczeństwa cyberprzestrzeni RP.

Pracownicy MAiC uczestniczyli w następujących ćwiczeniach:

- Cyber-EXE Polska 2014, organizowanych przez RCB, Fundację Bezpieczna Cyberprzestrzeń i firmę Deloitte. MAiC brało udział, jako uczestnik specjalny, niezaangażowany bezpośrednio w ćwiczenia;
- Cyber Europe 2014, organizowanych przez ENISA⁴². MAiC uczestniczyło w ćwiczeniach jako: podmiot odpowiadający za organizację ćwiczenia w Polsce, moderator ćwiczenia, podmiot monitorujący, gracz realizujący zadania wynikające ze scenariusza, punkt kontaktowy odpowiadający za współpracę z partnerami międzynarodowymi.

Z udzielonych wyjaśnień wynika, że poza dwoma ww. ćwiczeniami, MAiC nie otrzymywało zaproszeń do udziału w tego typu wydarzeniach.

(dowód: akta kontroli tom I str. 367-374)

W MAiC nie wypracowano założeń określających pożądany model testów penetracyjnych mających na celu weryfikację prawidłowości rozwiązań w zakresie bezpieczeństwa teleinformatycznego. Ministerstwo nie dysponowało również wiedzą na temat skali testów penetracyjnych prowadzonych w jednostkach administracji państwowej przez rządowe Zespoły CERT oraz przez podmioty komercyjne.

Podsekretarz Stanu w MAiC – Pan Roman Dmowski wyjaśnił, m.in. że *Polityka* nie określa żadnych wymagań w tym zakresie, a dodatkowo jest dokumentem o charakterze strategiczno-programowym i nie formułuje wprost obowiązków tego typu dla Ministra Administracji i Cyfryzacji.

(dowód: akta kontroli tom I str. 367-370)

⁴² Europejska Agencja Bezpieczeństwa Sieci i Informacji.

System wczesnego ostrzegania

Minister Administracji i Cyfryzacji nie uczestniczył w planowaniu oraz w realizacji projektu dotyczącego budowy i rozwoju systemu wczesnego ostrzegania o zdarzeniach w sieci Internet – ARAKIS. W MAiC nie dysponowano również wiedzą na temat zaplanowanych oraz osiągniętych celów i mierników tego projektu.

Podsekretarz Stanu w MAiC – Pan Roman Dmowski wskazał, że instytucjami właściwymi do kontaktów w sprawie projektu ARAKIS są ABW oraz Naukowa i Akademicka Sieć Komputerowa. Wyjaśnił, że plany rozwoju ww. systemu nie znajdują się w kompetencji MAiC, a dodatkową przyczyną braku aktywności Ministerstwa w tym obszarze jest brak zasobów.

(dowód: akta kontroli tom I str. 175)

Szkolenia i działania edukacyjne.

Podsekretarz Stanu w MAiC – Pan Roman Dmowski wyjaśnił, że MAiC nie dysponuje danymi pozwalającymi w sposób precyzyjny udzielić odpowiedzi na pytanie, czy w Polsce istnieje odpowiednia liczba specjalistów posiadających wystarczające kwalifikacje w obszarze ochrony cyberprzestrzeni. Zeznał, że w jego ocenie, w wyniku zamrożenia poziomu wynagrodzeń, w administracji nie ma możliwości zatrudnienia najwyższej klasy specjalistów od cyberbezpieczeństwa, a zatrudnienie średniej klasy specjalistów jest problematyczne.

Odnosnie wydawania przez MAiC wytycznych dla innych podmiotów publicznych dotyczących systemów zachęt, mających na celu pozyskanie i utrzymanie pracowników o niezbędnych kwalifikacjach w obszarze ochrony cyberprzestrzeni, zeznał: Nie znam innego systemu, który gruntownie rozwiązałby problem zbyt niskich wynagrodzeń i braku etatów. Nie widzę mechanizmów, które można by zarekomendować, żeby gruntownie zmieniały tę sytuację. Pewnym rozwiązaniem, ale nie idealnym jest pozyskiwanie specjalistów, w ramach usług świadczonych przez firmę zewnętrzną.

(dowód: akta kontroli tom I str. 176-179, tom III str. 473-474)

W zakresie budowy systemu szkoleń dotyczących bezpieczeństwa teleinformatycznego, w MAiC prowadzone były prace związane z programem szkoleń pełnomocników ds. ochrony cyberprzestrzeni oraz identyfikowaniem potrzeb szkoleniowych administracji państwowej. Ministerstwo nie podejmowało działań mających na celu wprowadzenie obowiązku przeprowadzania szkoleń w zakresie bezpieczeństwa IT (w szczególności dla pracowników administracji państwowej).

W okresie objętym kontrolą, MAiC zorganizowało następujące przedsięwzięcia szkoleniowe dotyczące bezpieczeństwa cyberprzestrzeni:

- seminarium *Bezpieczeństwo teleinformatyczne jako element integrujący systemy teleinformatyczne administracji* – w dniu 24 marca 2014 r. – w trakcie seminarium omawiano m.in. praktyczne aspekty dotyczące bezpieczeństwa teleinformatycznego na przykładzie MSZ;
- konferencja dla pełnomocników ds. bezpieczeństwa cyberprzestrzeni RP – w dniach 22-23 września 2014 r. – tematem konferencji, w której uczestniczyły 64 osoby były m.in. praktyczne aspekty bezpieczeństwa platformy Windows omówione przez przedstawicieli firmy Microsoft;
- szkolenie *Reagowanie na incydenty komputerowe w urzędach administracji rządowej*, zorganizowane w dniu 4 grudnia 2014 r. przy współpracy z ABW.

(dowód: akta kontroli tom I str. 176-179, 230-232, 266-269, tom III str. 380-382, tom IV str. 279-295)

MAiC nie opracowało i nie uczestniczyło w opracowaniu założeń kampanii informacyjno-edukacyjnych prowadzonych przez inne instytucje, dotyczących zagrożeń występujących w cyberprzestrzeni i metod zabezpieczenia przed nimi. Ministerstwo nie było również organizatorem tego rodzaju kampanii. Podsekretarz Stanu w MAiC – Pan Roman Dmowski wyjaśnił, że brak aktywności w ww. zakresie wynikał z niewystarczających zasobów kadrowych.

(dowód: akta kontroli tom I str. 179-180)

Minister Administracji i Cyfryzacji wspierał inicjatywy społeczne mające na celu realizację zadań związanych z ochroną cyberprzestrzeni RP. Wg stanu na dzień 30 września 2014 r., w wyniku konkursów przeprowadzonych na podstawie ustawy o działalności pożytku publicznego i o wolontariacie udzielono 4 dotacji⁴³ na prowadzenie kampanii społecznych o charakterze edukacyjno-prewencyjnym dotyczących korzystania z Internetu i bezpieczeństwa w cyberprzestrzeni. W dniu 16 października 2014 r. komisja konkursowa rekomendowała Ministrowi zawarcie 4 kolejnych umów dotacji⁴⁴ na realizację zadania publicznego pn. *Działania na rzecz poprawy poczucia bezpieczeństwa w środowisku cyfrowym poprzez rozwijanie świadomości zagrożeń, kształtowanie odpowiednich postaw oraz rozwijanie umiejętności wykorzystywania dostępnych narzędzi.*

(dowód: akta kontroli tom I str. 180, 270-287)

Wspieranie badań i rozwoju w obszarze ochrony cyberprzestrzeni.

W okresie objętym kontrolą, Minister Administracji i Cyfryzacji nie składał propozycji tematów naukowo-badawczych dotyczących ochrony cyberprzestrzeni RP.

MAiC było jednym z uczestników inicjatywy badawczej realizowanej przez konsorcjum, którego liderem jest Wojskowy Instytut Łączności, dotyczącej *Systemu ewaluacji zagrożeń bezpieczeństwa cyberprzestrzeni RP na potrzeby systemu zarządzania bezpieczeństwem narodowym Rzeczypospolitej Polskiej*. Pracownicy MAiC brali udział w Komitecie monitorującym postępy projektu.

Podsekretarz Stanu w MAiC – Pan Roman Dmowski wyjaśnił, że szczegółowe informacje o wydatkach poniesionych na realizację projektu mogą być udostępnione przez wykonawcę i podmiot finansujący, tj. Narodowe Centrum Badań i Rozwoju.

(dowód: akta kontroli tom I str. 84-119, 180, 288-293)

Współpraca międzynarodowa.

Minister Administracji i Cyfryzacji, we współpracy ze Stałym Przedstawicielstwem RP przy UE, aktywnie uczestniczył w pracach instytucji UE, związanych z przygotowaniem projektu dyrektywy NIS. W trakcie ww. prac, strona polska wspierała wprowadzenie realnych mechanizmów współpracy operacyjnej między państwami UE w zakresie bezpieczeństwa cyberprzestrzeni oraz sprzeciwiała się działaniom grupy państw członkowskich, zmierzającym do radykalnego ograniczenia zakresu oddziaływania tworzonej regulacji. Wspierana przez stronę polską koncepcja dyrektywy opierała się na tzw. modelu mieszanym, tj. zakładającym pewien stopień dobrowolności w budowie zdolności państw członkowskich w dziedzinie bezpieczeństwa sieci i informacji, z zachowaniem wymogów regulacyjnych wobec administracji publicznej i operatorów infrastruktury krytycznej.

(dowód: akta kontroli tom V str. 164-423)

Ustalone
nieprawidłowości

1. Ustalono, iż od momentu utworzenia Ministerstwa, do końca okresu objętego kontrolą, w MAiC nie określono w sposób rzetelny i kompleksowy, jakie zadania powinny być realizowane przez Ministra Administracji i Cyfryzacji w związku

⁴³ W ramach umów dotacji wydatkowano kwotę 686,5 tys. zł.

⁴⁴ Na łączną kwotę 838,9 tys. zł.

z ochroną cyberprzestrzeni RP. Powyższe skutkowało brakiem realizacji lub niewłaściwym wykonywaniem obowiązków, np. w zakresie kontroli wymienionych w art. 25 ustawy o informatyzacji, czy uzgodnienia Krajowego Planu Zarządzania Kryzysowego. W ocenie NIK, nie można uznać za zasadne wyjaśnień Kierownictwa MAiC wskazujących, że zadania Ministra w zakresie ochrony cyberprzestrzeni ograniczają się do realizacji *Polityki* i nie są one bezpośrednio związane z innymi regulacjami dotyczącymi zarządzania kryzysowego, prawa telekomunikacyjnego, czy interoperacyjności. Zdaniem NIK, obowiązki Ministra Administracji i Cyfryzacji wynikają bezpośrednio z faktu kierowania działami administracji rządowej informatyzacja oraz łączność i obejmują kompleksowe działania związane z bezpieczeństwem teleinformatycznym państwa.

2. W całym okresie objętym badaniem, Minister Administracji i Cyfryzacji nie realizował obowiązków kontrolnych wymienionych w art. 25 ust. 1 pkt 3 lit. b) i c) ustawy o informatyzacji, a działania organizacyjne polegające na przygotowaniu kadr Ministerstwa do realizacji tych zadań zostały podjęte dopiero po kontroli NIK dotyczącej krajowych ram interoperacyjności. W ocenie NIK, nie można uznać udzielonych wyjaśnień, że brak formalnej ewidencji systemów wykorzystywanych do realizacji zadań publicznych całkowicie uniemożliwia realizację obowiązków kontrolnych. Należy podkreślić, że Minister Administracji i Cyfryzacji dysponował różnymi możliwościami i źródłami pozyskiwania danych w ww. zakresie, w tym w szczególności od jednostek podległych i nadzorowanych. Np. ewidencja kilkuset systemów teleinformatycznych wykorzystywanych do realizacji zadań publicznych została opracowana w wyniku przeprowadzonego w 2013 r. audytu wewnętrznego i przekazana w formie elektronicznej do MAiC. Informacje o systemach administracji publicznej są również dostępne na stronach internetowych GUS⁴⁵. Całkowite odstępianie od przeprowadzania kontroli świadczy natomiast o tolerowaniu sytuacji niesposobienia przepisów i braku wykorzystania gotowych rozwiązań ustawowych do realizacji zadań związanych z ochroną cyberprzestrzeni państwa.
3. Kontrola wykazała, że Minister Administracji i Cyfryzacji w praktyce nie inicjował i nie koordynował działań innych podmiotów państwowych związanych z ochroną cyberprzestrzeni oraz w ogóle nie realizował zadań związanych z koordynacją krajowego systemu reagowania na incydenty komputerowe w cyberprzestrzeni RP. Wprawdzie, od stycznia 2014 r., podjęto działania dotyczące np. organizacji szkoleń, ewidencjonowania danych pełnomocników ds. bezpieczeństwa cyberprzestrzeni, czy udziału w ćwiczeniach, to jednak zakres realizowanych zadań był bardzo ograniczony w stosunku do faktycznych zadań Ministra Administracji i Cyfryzacji związanych z bezpieczeństwem teleinformatycznym państwa.

Odpowiedzialność za opisane powyżej nieprawidłowości ponoszą osoby zajmujące w latach 2011 – 2014 stanowisko Ministra Administracji i Cyfryzacji oraz Pan Roman Dmowski – Podsekretarz Stanu w MAiC, któremu od września 2013 r. powierzono zadania związane z ochroną cyberprzestrzeni RP.

Ocena częściowa

Najwyższa Izba Kontroli ocenia negatywnie dotychczasową działalność Ministra Administracji i Cyfryzacji w zakresie realizacji zadań związanych z ochroną cyberprzestrzeni RP.

⁴⁵ <http://bip.stat.gov.pl/dzialalnosc-statystyki-publicznej/polska-statystyka-publiczna/>

IV. Wnioski

Wnioski pokontrolne

Przedstawiając powyższe oceny i uwagi wynikające z ustaleń kontroli, Najwyższa Izba Kontroli, na podstawie art. 53 ust. 1 pkt 5 ustawy z dnia 23 grudnia 1994 r. o Najwyższej Izbie Kontroli⁴⁶, wnosi o:

1. Przeprowadzenie, w trybie pilnym, kompleksowej analizy zadań Ministra Administracji i Cyfryzacji związanych z ochroną cyberprzestrzeni RP, obejmującej m.in. kwerendę aktów prawnych dotyczących bezpieczeństwa teleinformatycznego oraz inwentaryzację kluczowych, państwowych zasobów IT, które powinny być poddane szczególnej ochronie.
2. Rzetelne oszacowanie zasobów (ludzkich, finansowych i rzeczowych) Ministerstwa oraz innych instytucji państwowych niezbędnych do budowy i skutecznego funkcjonowania krajowego systemu ochrony cyberprzestrzeni.
3. Poinformowanie, w trybie pilnym, Prezesa Rady Ministrów o faktycznych uwarunkowaniach i ograniczeniach realizacji zadań Ministra Administracji i Cyfryzacji związanych z bezpieczeństwem teleinformatycznym, w celu podjęcia wiążących, strategicznych decyzji dotyczących kształtu systemu ochrony cyberprzestrzeni w Polsce oraz źródeł jego finansowania.
4. Bezwzględne podjęcie działań organizacyjnych w celu ustanowienia w MAiC ośrodka koordynacji działań związanych z ochroną cyberprzestrzeni RP oraz krajowego systemu reagowania na incydenty komputerowe, będącego w stanie zarządzać aktualnymi zagrożeniami w cyberprzestrzeni, do czasu wdrożenia docelowego, kompleksowego systemu bezpieczeństwa teleinformatycznego państwa.

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 Prezesa Najwyższej Izby Kontroli.

Obowiązek
poinformowania
NIK o sposobie
wykorzystania uwag
i wykonania wniosków

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

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

Warszawa, dnia 22 stycznia 2015 r.

Wiceprezes
Najwyższej Izby Kontroli
Wojciech Kutyla



⁴⁶ Dz. U. z 2012 r., poz.82 ze zm.