WICEPREZES
NAJWYŻSZEJ IZBY KONTROLI
Wojciech Kutyła

KPB – 4101-002-03/2014
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 (cyberprzestrzeni RP).
Jednostka przeprowadzająca kontrolę	Najwyższa Izba Kontroli Departament Porządku i Bezpieczeństwa Wewnętrznego
Kontroler	Adam Czugajewicz, specjalista k. p., upoważnienie do kontroli nr 89664 z 2 czerwca 2014 r. (dowód: akta kontroli str. 1-2)
Jednostka kontrolowana	Ministerstwo Spraw Wewnętrznych (zwane dalej MSW), ul. Batorego 5, Warszawa (02-591)
Kierownik jednostki kontrolowanej	Minister Spraw Wewnętrznych: - Jacek Cichocki – od 18 listopada 2011 r. do 25 lutego 2013 r.; - Bartłomiej Sienkiewicz – od 25 lutego 2013 r. do 22 września 2014 r.. (dowód: akta kontroli str. 244-245)

II. Ocena kontrolowanej działalności

Ocena ogólna

Kontrola wykazała[1], że Minister Spraw Wewnętrznych[2] nie uczestniczył aktywnie w budowie i wdrażaniu systemu ochrony cyberprzestrzeni RP. Od momentu utworzenia Ministerstwa w listopadzie 2011 r., MSW nie realizowało w praktyce żadnych zadań związanych z ochroną cyberprzestrzeni skierowanych na zewnątrz, a działania w tym zakresie ograniczone były do własnych sieci i systemów resortowych. Stwierdzono również, że działania Ministerstwa nie miały charakteru systemowego i nie uwzględniały obowiązków i wytycznych wynikających z *Polityki Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej*[3] (zwanej dalej *Polityką*). W szczególności: nie oszacowano zasobów niezbędnych do realizacji zadań związanych z ochroną cyberprzestrzeni, nie opracowano procedur bezpieczeństwa teleinformatycznego resortu, nie powołano pełnomocnika ds. bezpieczeństwa cyberprzestrzeni oraz nie zrealizowano zapisów *Polityki* dotyczących oszacowania ryzyka dla systemów teleinformatycznych wykorzystywanych przez Ministerstwo. Nie realizowano także obowiązków wynikających z art. 25 ust. 1 pkt 3 lit. b ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne[4], dotyczących kontroli systemów teleinformatycznych, a Minister nie posiadał pełnej wiedzy o rzeczywistej liczbie systemów podlegających jego kontroli. Działania związane z realizacją zadań wynikających z *Polityki* zostały podjęte przez MSW dopiero w trakcie kontroli NIK.

---

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.

2 Kontrolą objęto okres od dnia utworzenia Ministerstwa Spraw Wewnętrznych (18 listopada 2011 r.) do dnia zakończenia czynności kontrolnych (29 sierpnia 2014 r.)

3 Przyjętej uchwałą Rady Ministrów nr 111/2013 z dnia 25 czerwca 2013 r.

4 Dz. U. z 2014 r., poz. 1114.

W ocenie NIK, niekorzystny wpływ na realizację zadań w zakresie ochrony cyberprzestrzeni wywierały zmiany organizacyjne i kadrowe w MSW, w tym zmniejszenie liczebności komórki ds. bezpieczeństwa teleinformatycznego oraz obniżenie poziomu kwalifikacji zatrudnionych w niej osób.

III. Wyniki kontroli

1. Działania Ministra Spraw Wewnętrznych w ramach budowy systemu ochrony cyberprzestrzeni RP.

Opis stanu faktycznego

1.1 Określenie ram prawnych systemu ochrony cyberprzestrzeni RP.

W ramach opracowania wykazu propozycji legislacyjnych koniecznych do wprowadzenia w celu wdrożenia systemu ochrony cyberprzestrzeni RP w MSW podjęto następujące działania:

- w trakcie kontroli opracowano projekt zarządzenia Ministra Spraw Wewnętrznych powołującego pełnomocnika ds. ochrony cyberprzestrzeni oraz rozpoczęto prace nad założeniami do projektu zarządzenia Ministra Spraw Wewnętrznych w sprawie organizacji i funkcjonowania systemu reagowania na incydenty komputerowe w resorcie spraw wewnętrznych;
- w trakcie kontroli prowadzono przegląd obecnie obowiązujących regulacji prawnych w celu przygotowania rozwiązań zwiększających poziom bezpieczeństwa cyberprzestrzeni, obejmujący analizę ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne, rozporządzenie Rady Ministrów w sprawie Krajowych Ram Interoperacyjności[5] oraz *Polityki* w celu dostosowania do nich rozwiązań organizacyjno-funkcjonalnych i regulacji wewnętrznych MSW.

MSW, w okresie objętym kontrolą, nie inicjowało działań legislacyjnych w związku z koniecznością unormowania zadań związanych z ochroną cyberprzestrzeni RP.

W ocenie Ministra Spraw Wewnętrznych inicjatywa podejmowania działań legislacyjnych dających podstawy do wdrożenia zapisów pkt. 3.3. *Polityki* należy do Rady Ministrów i ministra właściwego ds. informatyzacji. Jako priorytetowy kierunek zmian legislacyjnych Minister wskazał opracowanie przepisów ustawowych, normujących wprost kwestie finansowania realizacji *Polityki* oraz samej ochrony cyberprzestrzeni na wielu płaszczyznach życia gospodarczego i społecznego.

(dowód: str. 58-61, 68-73, 179-203)

Od 2009 r. Komendant Główny Policji kierował do Ministra Spraw Wewnętrznych i Administracji, a następnie Ministra Spraw Wewnętrznych pisma postulujące zmiany legislacyjne, m. in. w ustawie z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną, w związku ze wzrostem przestępczości internetowej. Ostatnie pismo w tej sprawie zostało skierowane do MSW 28 maja 2014 r. Minister Spraw Wewnętrznych wyjaśnił, że właściwy do zainicjowania zmian w ww. ustawie jest Minister Administracji i Cyfryzacji, *(...) a MSW rozważy wystąpienie z wnioskiem do MAiC o podjęcie stosownej inicjatywy legislacyjnej.*

(dowód: str. 181-187)

Od 28 lutego do 31 października 2013 r. w MSW prowadzone były prace związane z opiniowaniem projektu zmiany zarządzenia Nr 74 Prezesa Rady Ministrów z dnia

---

[5] Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz. U. z 2012 r., poz. 526.).

12 października 2011 r. w sprawie wykazu przedsięwzięć i procedur systemu zarządzania kryzysowego, wprowadzającego m.in. odrębne stopnie alarmowe związane z zagrożeniami występującymi w cyberprzestrzeni. MSW przekazało Rządowemu Centrum Bezpieczeństwa (RCB) uwagi do ww. projektu pismami z 9 kwietnia i 31 października 2013 r.

(dowód: str. 181-187)

MSW nie zawierało umów lub porozumień z innymi podmiotami dotyczących realizacji zadań związanych z ochroną cyberprzestrzeni RP.

(dowód: str. 68-73)

MSW nie przekazywało dokumentacji wytworzonej w okresie wcześniejszym w Ministerstwie Spraw Wewnętrznych i Administracji w związku z realizacją zadań związanych z ochroną cyberprzestrzeni do nowo utworzonego Ministerstwa Administracji i Cyfryzacji (MAiC).

(dowód: str. 175-176, 181-187)

1.2 Szacowanie ryzyk związanych ze zdarzeniami występującymi w cyberprzestrzeni.

W MSW nie został zrealizowany obowiązek wynikający z pkt. 3.1. *Polityki* dotyczący przeprowadzenia szacowania ryzyka związanego z funkcjonowaniem cyberprzestrzeni w zakresie systemów teleinformatycznych wykorzystywanych przez Ministerstwo[6]. Z udzielonych wyjaśnień wynika, że działania mające na celu oszacowanie ryzyka zostały rozpoczęte w trakcie kontroli NIK, natomiast kontrolującemu nie przedstawiono żadnej dokumentacji wytworzonej w związku z ww. procesem. Jak wyjaśnił Minister Spraw Wewnętrznych zakończenie szacowania ryzyka przewidziane jest na koniec 2014 r.

MSW nie prowadziło współpracy z MAiC lub RCB mającej na celu opracowywanie jednolitej metodyki, zapewniającej porównywalność i komplementarność wyników szacowania ryzyka związanego ze zdarzeniami występującymi w cyberprzestrzeni z procesem szacowania ryzyka realizowanym na podstawie regulacji dotyczących zarządzania kryzysowego.

(dowód: str. 17-22, 181-187)

W okresie objętym kontrolą MSW analizowało przykładowe ryzyka i zagrożenia dla systemów teleinformatycznych resortu w dokumentach sporządzanych na podstawie ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym[7], tj.:

- w zaktualizowanym raporcie cząstkowym Ministra Spraw Wewnętrznych o zagrożeniach bezpieczeństwa narodowego przekazanym do RCB w dniu 31 sierpnia 2012 r. zdefiniowano zagrożenia dotyczące: ujawnienia lub utraty informacji niejawnych przetwarzanych w systemach teleinformatycznych, braku funkcjonowania sieci GovNet, Systemu Rejestrów Państwowych, CEPiK, Paszportowego Systemu Informacyjnego, awarii lub uszkodzenia Centralnego Węzła Teleinformatycznego Straży Granicznej;
- w dokumentacji przygotowanej na potrzebę opracowania Narodowego Programu Ochrony Infrastruktury Krytycznej wskazano ryzyka dla systemów teleinformatycznych Policji, Straży Granicznej i Państwowej Straży Pożarnej.

(dowód: str. 17-22, 273)

---

[6] Zgodnie z pkt 3.1. *Polityki* wyniki szacowania ryzyka powinny zostać przekazane ministrowi właściwemu ds. informatyzacji w terminie do 31 stycznia każdego roku. Zgodnie z terminem wyznaczonym przez MAiC szacowanie ryzyka za 2013 r. (pierwszy rok obowiązywania *Polityki*) miało być przeprowadzone do końca marca 2014 r.

[7] Dz. U. z 2013 r., poz. 1166.

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

W okresie od utworzenia MSW do 31 grudnia 2012 r. zadania związane z ochroną cyberprzestrzeni, zgodnie z zarządzeniem nr 27 Dyrektora Generalnego MSW z 23 grudnia 2011 r. w sprawie zatwierdzenia wewnętrznego regulaminu Departamentu Ewidencji Państwowych i Teleinformatyki (DEPiT), należały do właściwości tego Departamentu. Zadania te obejmowały m. in.:

- prowadzenie spraw związanych z obsługą incydentów teleinformatycznych i zapewnieniem bezpieczeństwa informacji w systemach informatycznych MSW;
- współpracę ze służbami dyżurnymi jednostek organizacyjnych podległych MSW oraz Szefem Agencji Bezpieczeństwa Wewnętrznego (ABW) i zespołem reagowania na incydenty teleinformatyczne (CERT) w zakresie monitorowania i zapobiegania incydentom dotyczącym bezpieczeństwa systemów teleinformatycznych;
- współpracę z organami innych państw i instytucjami UE w obszarze ochrony teleinformatycznej i infrastruktury krytycznej;
- przeciwdziałanie zagrożeniom wewnętrznym i zewnętrznym, w tym cyberterroryzmowi i ochronę teleinformatycznej infrastruktury krytycznej;
- prowadzenie spraw związanych z organizacją i koordynacją zadań w zakresie bezpieczeństwa teleinformatycznego i ochrony danych osobowych przetwarzanych w sieciach i systemach teleinformatycznych MSW;
- realizację działań związanych z opracowaniem strategii i polityk ochrony cyberprzestrzeni RP.

Od 1 stycznia 2013 r., na podstawie zarządzenia nr 111 Prezesa Rady Ministrów z 20 grudnia 2012 r. zmieniającego statut MSW, ww. zadania związane z ochroną cyberprzestrzeni przekazano do właściwości dwóch komórek organizacyjnych nowo utworzonego Departamentu Teleinformatyki (DT): Wydziału Utrzymania Sieci i Zespołu ds. Bezpieczeństwa.

Zadania związane z ochroną cyberprzestrzeni realizowały również:

- Departament Strategii i Analiz - w zakresie opracowania i opiniowania standardów i polityk bezpieczeństwa związanych z bezpieczeństwem informacji;
- Wydział Komunikacji w Biurze Ministra[8] - poprzez bieżący nadzór nad funkcjonowaniem i bezpieczeństwem serwerów internetowych oraz monitorowanie umowy z firmą utrzymującą serwery w sieci Internet;
- wyznaczeni pracownicy Wydziału Informatyki i Łączności Biura Administracyjno-Finansowego - poprzez administrowanie systemami informatycznymi i współpracę z CERT.

Ponadto, Dyrektor Generalny MSW decyzją nr 5 z 23 kwietnia 2013 r. powołał Zespół ds. Bezpieczeństwa Teleinformatycznego MSW, którego zadaniem jest opracowanie Polityki Bezpieczeństwa Informacji MSW.

(dowód: str. 5-6, 10-16, 41-48)

W ramach struktury organizacyjnej obowiązującej do końca 2012 r., zadania z zakresu ochrony cyberprzestrzeni w MSW realizował głównie Wydział Standardów i Polityk Bezpieczeństwa DEPiT. Wg stanu na dzień 31 grudnia 2012 r. ww. Wydział

[8] Od 2 lipca 2013 r. Biuro Komunikacji Społecznej.

liczył 10 pracowników, posiadających ukończone studia i szkolenia specjalistyczne w zakresie m.in. informatyki, elektrotechniki, testów penetracyjnych oraz bezpieczeństwa systemów teleinformatycznych. Po przeprowadzeniu zmian organizacyjnych, w miejsce ww. Wydziału utworzono Zespół ds. Bezpieczeństwa DT liczący 3 pracowników, w którym brak jest osób z wykształceniem informatycznym[9].

(dowód: str. 25-29, 31-39, 65-67, 171-172, 179-180)

W ocenie pracowników MSW zajmujących się kwestiami bezpieczeństwa teleinformatycznego, istnieje potrzeba przywrócenia komórki zajmującej się *stricte* kwestiami bezpieczeństwa teleinformatycznego w MSW, zaś liczebność takiej komórki w zależności od założonego poziomu bezpieczeństwa powinna wynosić od 5 do 20 osób.

(dowód: str. 25-29, 31-39, 65-67)

Od utworzenia MSW, tj. w ciągu 3 lat, zadania dotyczące teleinformatyki MSW leżały w gestii 4 podsekretarzy stanu, 6 zastępców dyrektora DEPiT oraz 4 dyrektorów i zastępców dyrektora DT.

(dowód: str. 244-245)

Z wyjaśnień udzielonych przez Ministra wynika, że w latach 2012-2014 MSW nie ponosiło wydatków na realizację zadań związanych z ochroną cyberprzestrzeni. Ustalono natomiast, że wg stanu na dzień zakończenia kontroli w MSW nie przeprowadzono kompleksowego szacowania zasobów oraz wydatków związanych z ochroną cyberprzestrzeni RP. Kierownictwo Ministerstwa nie dysponowało również rzetelnymi i precyzyjnymi danymi na temat liczby pracowników zaangażowanych w realizację ww. działań oraz przypisanych im zadań. W związku z powyższym w MSW nie zrealizowano obowiązków określonych w pkt 5 *Polityki* dotyczących przekazania Ministrowi Administracji i Cyfryzacji (po zatwierdzeniu tego dokumentu) informacji na temat wykonanych dotychczas zadań związanych z ochroną cyberprzestrzeni oraz wydatków poniesionych na ich realizację. Nie przekazywano również ww. podmiotowi informacji na temat wydatków planowanych do poniesienia w latach kolejnych.

Z udzielonych wyjaśnień wynika, że ww. zadania nie zostały zrealizowane, ponieważ określenie zasobów i wydatków jest zależne od wyników szacowania ryzyka, wymienionego w pkt 3.1. *Polityki*, które nie zostało dotychczas przeprowadzone dla systemów teleinformatycznych MSW (brak realizacji obowiązku dotyczącego szacowania ryzyka szczegółowo opisano w pkt III.1.1.2 wystąpienia pokontrolnego).

Minister wskazał, że prace mające na celu oszacowanie ryzyka są w toku, a następnie zostanie przeprowadzona analiza kosztów realizacji zadań.

(dowód: str. 5-6, 10-16, 41-48, 58-61, 68-73,241-243)

W MSW nie powołano pełnomocnika ds. bezpieczeństwa cyberprzestrzeni[10], jak również nie podejmowano działań w celu upowszechniania tej funkcji w jednostkach podległych lub nadzorowanych. Minister wyjaśnił, że zostanie zainicjowany proces legislacyjny mający na celu powołanie pełnomocnika ds. bezpieczeństwa cyberprzestrzeni.

(dowód: str. 5-6, 10-22, 179-187, 188-190)

---

[9] W skład zespołu weszło 2 pracowników dotychczasowego Wydział Standardów i Polityk Bezpieczeństwa z wykształceniem elektrotechnicznym oraz 1 pracownik zatrudniony w maju 2014 r., nie posiadający kwalifikacji i doświadczenia zawodowego związanego z teleinformatyką. Z udzielonych wyjaśnień wynika, że ww. osoba planuje w roku akademickim 2014/2015 rozpocząć studia podyplomowe z zakresu bezpieczeństwa systemów teleinformatycznych.

[10] Zasadność powołania w poszczególnych jednostkach administracji rządowej pełnomocnika ds. bezpieczeństwa cyberprzestrzeni została wskazana w pkt 3.4.3. *Polityki*.

1.4 Opracowanie mierników oraz projektów szczegółowych określających sposób realizacji zadań w ramach ochrony cyberprzestrzeni RP.

Zgodnie z pkt. 6 *Polityki* jednostki administracji rządowej były zobowiązane przekazać Ministrowi Administracji i Cyfryzacji, w ciągu roku od przyjęcia *Polityki*, informacje o przyjętych i osiągniętych przez nie procentowych wskaźnikach realizacji zadań wynikających z wdrażania tego dokumentu.

MSW nie opracowało i nie przekazało do MAiC ww. wskaźników. Jak wyjaśnił Minister, nie zrealizowano ww. obowiązku, ponieważ nie zostało dotychczas przeprowadzone szacowanie ryzyka dla systemów teleinformatycznych MSW, którego wyniki, w ocenie Ministerstwa, są niezbędne dla prawidłowego określenia wskaźników realizacji zadań.

(dowód: str. 23-24, 55-61, 68-73)

W okresie objętym kontrolą MSW nie opracowało i nie uczestniczyło w opracowaniu projektów szczegółowych dotyczących celów i założeń *Polityki*.

(dowód: str. 58-61, 68-73)

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

Z udzielonych wyjaśnień wynika, że w ramach krajowego systemu reagowania na incydenty komputerowe MSW realizuje zadania przypisane dla Poziomu III tego systemu, tj. poziomu realizacji, w ramach którego administratorzy odpowiadają za poszczególne systemy teleinformatyczne funkcjonujące w cyberprzestrzeni.

W MSW wykorzystywana jest klasyfikacja incydentów komputerowych określonych w formularzu zgłoszenia incydentu Rządowego Zespołu Reagowania na Incydenty Komputerowe (CERT.GOV.PL).

(dowód: str. 5-6, 10-16)

Działania MSW w ramach wspierania budowy sytemu wymiany informacji polegały na przyłączeniu się do systemu wczesnego ostrzegania ARAKIS-GOV poprzez instalację sondy w sieciach i systemach MSW oraz udostępnienie części publicznej adresacji IP.

Jednostki podległe i nadzorowane przez MSW nie były zobligowane do przekazywania do MSW informacji o incydentach w cyberprzestrzeni. Minister wyjaśnił, że rozważana jest możliwość wprowadzenia takiego obowiązku w projekcie zarządzenia w sprawie powołania pełnomocnika Ministra do spraw bezpieczeństwa cyberprzestrzeni.

(dowód: str. 5-6, 10-16, 241-243)

Ustalone nieprawidłowości

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

Ustalono, iż w ciągu roku od przyjęcia przez Radę Ministrów *Polityki Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej*, w MSW nie prowadzono praktycznie żadnych działań mających na celu wdrożenie postanowień ww. dokumentu. Nie zrealizowano podstawowego zadania, określonego w pkt 3.1. *Polityki*, dotyczącego oszacowania ryzyka dla systemów teleinformatycznych Ministerstwa oraz nie wykonano obowiązków wymienionych w pkt 5. i 6. tego dokumentu w zakresie przekazania Ministrowi Administracji i Cyfryzacji informacji na temat wydatków poniesionych i planowanych w związku z ochroną cyberprzestrzeni oraz przyjętych przez MSW w tym obszarze wskaźników realizacji zadań.

Działania mające na celu realizację postanowień *Polityki* zostały rozpoczęte dopiero w trakcie kontroli NIK.

Odpowiedzialność za powstanie opisanych powyżej nieprawidłowości ponoszą osoby zajmujące w okresie objętym kontrolą stanowisko Ministra Spraw Wewnętrznych oraz Członkowie Kierownictwa Ministerstwa sprawujący nadzór nad realizacją zadań związanych z ochroną cyberprzestrzeni RP.

Uwagi dotyczące badanej działalności

NIK zwraca uwagę, iż brak oszacowania zasobów oraz wydatków i wskaźników realizacji zadań Ministerstwa w zakresie bezpieczeństwa teleinformatycznego, wskazują na istotny problem związany ze zdefiniowaniem faktycznej roli Ministra Spraw Wewnętrznych w budowanym systemie ochrony cyberprzestrzeni RP. Zdaniem NIK, zadania MSW w ramach ww. systemu nie powinny ograniczać się do ochrony własnych sieci i systemów teleinformatycznych, co wynika w szczególności z przypisania Ministrowi odpowiedzialności za zarządzanie kryzysowe[11], którego integralnym elementem są zagadnienia ochrony teleinformatycznej infrastruktury krytycznej państwa. Ważną rolę MSW w ww. zakresie potwierdza także przyznanie Ministrowi Spraw Wewnętrznych funkcji Współprzewodniczącego nowo powołanego *Zespołu zadaniowego do spraw bezpieczeństwa cyberprzestrzeni Rzeczypospolitej Polskiej*[12]. W powyższym zakresie zasadne jest więc przeprowadzenie rzetelnej analizy, m.in. we współpracy z Ministrem Administracji i Cyfryzacji, w celu określenia zadań MSW w związku z ochroną cyberprzestrzeni RP oraz zasobów Ministerstwa niezbędnych do ich realizacji.

Ocena cząstkowa

Kontrola wykazała, że Minister Spraw Wewnętrznych nie uczestniczył aktywnie w budowie systemu ochrony cyberprzestrzeni RP. W okresie objętym badaniem, MSW nie inicjowało działań legislacyjnych, mających na celu unormowanie zagadnień związanych z ochroną teleinformatyczną państwa oraz nie zrealizowało zadań określonych w *Polityce* dotyczących oszacowania ryzyka oraz określenia wskaźników realizacji zadań w zakresie ochrony cyberprzestrzeni. Nie dokonano oszacowania zasobów – ludzkich i finansowych – niezbędnych do skutecznej realizacji zadań ww. obszarze, natomiast podczas kolejnych reorganizacji malała liczba i kwalifikacje pracowników Ministerstwa zajmujących się *stricte* kwestiami ochrony teleinformatycznej.

2. Działania Ministra Spraw Wewnętrznych w ramach ochrony cyberprzestrzeni RP.

2.1 Ustanowienie i kontrola podstawowych wymogów w zakresie bezpieczeństwa cyberprzestrzeni.

Opis stanu faktycznego

W MSW nie opracowano regulacji lub zaleceń dotyczących wymogów bezpieczeństwa systemów teleinformatycznych oraz systemu zarządzania bezpieczeństwem informacji. Dyrektor Generalny MSW decyzją nr 5 z 23 kwietnia 2013 r. powołał Zespół ds. Bezpieczeństwa Teleinformatycznego MSW, którego zadaniem jest opracowanie Polityki Bezpieczeństwa Informacji Ministerstwa, natomiast wg stanu na dzień 31 lipca 2014 r. ww. dokument nie został opracowany.

---

[11] Minister Spraw Wewnętrznych – zgodnie z § 1 ust. 2 rozporządzenia Prezesa Rady Ministrów z dnia 18 listopada 2011 r. w sprawie szczegółowego zakresu działania Ministra Spraw Wewnętrznych (Dz. U. Nr 248, poz. 1491) – kieruje działem administracji rządowej sprawy wewnętrzne obejmującym m.in. sprawy ochrony bezpieczeństwa i porządku publicznego oraz zarządzania kryzysowego.

[12] Ww. Zespół został powołany Decyzją Przewodniczącego Komitetu Rady Ministrów do spraw Cyfryzacji Nr/1/2014 z dnia 13 czerwca 2014 r., w związku z realizacją pkt. 3.4.1. *Polityki*.

Do dnia zakończenia czynności kontrolnych nie przedstawiono również sprawozdań z działalności Zespołu, które zgodnie z § 5 ww. decyzji powinny być sporządzane kwartalnie. Z wyjaśnień udzielonych przez Ministra wynika, że *w chwili obecnej trwa ustalanie w Departamencie Teleinformatyki, czy ww. sprawozdania były sporządzane.*

Stwierdzono także, że wiodącą rolę w przygotowaniu Polityki Bezpieczeństwa Informacji oraz Systemu Reagowania na Incydenty Komputerowe Ministerstwa powierzono pracownikowi nie posiadającemu kwalifikacji i doświadczenia zawodowego w zakresie teleinformatyki.

(dowód: str. 5-6, 10-16, 41-48, 58-61, 68-73, 179-180)

W całym okresie objętym kontrolą, Minister Spraw Wewnętrznych nie realizował, w stosunku do podmiotów podległych lub nadzorowanych obowiązków kontrolnych wymienionych w art. 25 ust. 1 pkt 3 lit. b ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne, w tym, w zakresie sprawdzenia minimalnych zabezpieczeń systemów teleinformatycznych wykorzystywanych przez te jednostki. Stwierdzono również, że w Ministerstwie nie dysponowano wiedzą na temat pełnej liczby i rodzaju systemów teleinformatycznych, podlegających kontroli Ministra Spraw Wewnętrznych na podstawie ww. przepisu.

Minister wyjaśnił, że nie przeprowadzano kontroli w ww. zakresie, ponieważ brak jest jednoznacznego zapisu wskazującego na częstotliwość kontroli. Wskazał również, że nie dysponowano odpowiednią liczbą osób posiadających certyfikaty uprawniające do przeprowadzania kontroli, o których mowa w art. 28 ustawy.

Minister poinformował, że kontroli MSW na podstawie ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne mogą podlegać w szczególności: Krajowy System Informacji Policji, Krajowy System Informatyczny, System Odprawa SG, Centralna Baza Danych Systemu Obsługi Cudzoziemców, System Centralnej Personalizacji Dokumentów, Paszportowy System Informacyjny, SWD-ST PSP, modułowe systemy medyczne SOLMED, KS-PPS, INFOMEDICA. Wyjaśnił, że nie określono pełnej liczby i rodzaju systemów teleinformatycznych, podlegających kontroli Ministra Spraw Wewnętrznych ze względu na dużą różnorodności systemów w jednostkach podległych i nadzorowanych. Poinformował, że zwrócono się do MAiC o skonkretyzowanie, jakie systemy informatyczne służące do realizacji zadań publicznych podlegają kontroli MSW.

(dowód: str. 17-18, 19-22, 58-61, 68-73, 181-187, 241-243)

2.2 Rozwój narodowych planów kryzysowych – ciągłości działania.

Minister Spraw Wewnętrznych wskazał, że obowiązujące w Polsce plany kryzysowe na wypadek zagrożeń dla systemów teleinformatycznych infrastruktury krytycznej zostały ujęte w Krajowym Planie Zarządzania Kryzysowego, opracowanym przez RCB, a opiniowanym m. in. przez MSW.

(dowód: str. 23-24, 55-57)

W części I Krajowego Planu Zarządzania Kryzysowego[13] (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 kryzysowego[14]. W związku z powyższym w ww. dokumencie w ogóle nie zawarto zadań i podmiotów odpowiedzialnych za zarządzanie zdarzeniami kryzysowymi występującymi w cyberprzestrzeni

[13] Wersja zaktualizowana, przyjęta na podstawie uchwały Rady Ministrów z 23 lipca 2013 roku.

[14] Zapobieganie, przygotowanie, reagowanie, odbudowa.

oraz pominięto wiodącą rolę Ministra Administracji i Cyfryzacji w zarządzaniu tymi zagrożeniami, wynikającą z kierowania działami administracji rządowej informatyzacja i łączność oraz z zapisów *Polityki.*

MSW nie podejmowało działań mających na celu aktualizację KPZK poprzez wskazanie w tym dokumencie zadań i podmiotów odpowiedzialnych za zarządzanie zdarzeniami kryzysowymi występującymi w cyberprzestrzeni.

Minister Spraw Wewnętrznych wyjaśnił, że: *Podczas opiniowania Krajowego Planu Zarządzania Kryzysowego zarówno komórki organizacyjne MSW właściwe w sprawach teleinformatyki, jak również służby MSW nie zgłaszały potrzeby uzupełnienia Planu o zagrożenia występujące w cyberprzestrzeni. Gdyby taka propozycja pojawiła się na którymkolwiek etapie wewnątrzresortowego opiniowania KPZK, MSW zgłosiłoby do RCB potrzebę umieszczenia (uzupełnienia) zagrożeń dotyczących cyberprzestrzeni.*

(dowód: str. 58-61, 68-73)

Ustalono, że w *Planie zarządzania kryzysowego działu administracji rządowej: sprawy wewnętrzne*[15]: zwarto dwie procedury reagowania na zagrożenia dla systemów teleinformatycznych MSW:

- *procedura realizacji zadania PRZ 5 – Zagrożenia dla funkcjonowania rejestrów państwowych i systemu wymiany informacji*;
- *Procedura realizacji zadania PRZ 6 – Zakłócenia w funkcjonowaniu systemów łączności.*

Opracowana została również *Instrukcja punktu kontaktowego komórki organizacyjnej MSW właściwej w sprawach łączności*, zatwierdzona 27 marca 2014 r. przez Dyrektora Departamentu Teleinformatyki.

(dowód: str. 5-6, 10-16, 246-270)

2.3 Organizacja ćwiczeń i testów systemu bezpieczeństwa cyberprzestrzeni.

MSW nie organizowało ani nie uczestniczyło w ćwiczeniach systemu bezpieczeństwa w cyberprzestrzeni.

(dowód: str. 5-6, 10-16, 58-61, 68-73)

2.4 Szkolenia i działania edukacyjne.

W okresie objętym kontrolą, pracownicy MSW odbyli następujące szkolenia dotyczące bezpieczeństwa teleinformatycznego[16]: *Przygotowanie dokumentacji bezpieczeństwa teleinformatycznego na podstawie nowych przepisów o ochronie informacji niejawnych* – 1 osoba, *Bezpieczeństwo aplikacji internetowych* - 1 osoba, *Specjalistyczne szkolenie dla administratorów systemu oraz inspektorów bezpieczeństwa teleinformatycznego* – 1 osoba, *Bezpieczeństwo teleinformatyczne dla administratorów systemu lub inspektorów bezpieczeństwa teleinformatycznego* – 2 osoby, *Analiza ryzyka dla informacji niejawnych przetwarzanych w systemie teleinformatycznym* – 3 osoby, *Administrator Bezpieczeństwa Informacji i Audytor Wewnętrzny SZBI wg ISO 27001* – 1 osoba, *Testy penetracyjne systemów IT* – 1 osoba. Dwie z osób uczestniczących w powyższych szkoleniach zostały wskazane przez Ministra jako pracownicy realizujący w MSW zadania z obszaru ochrony cyberprzestrzeni.

---

15 Dokument zatwierdzony w dniu 3 września 2013 r. przez Ministra Spraw Wewnętrznych.

16 Większość szkoleń trwała jeden dzień.

Ww. szkolenia nie zostały zaplanowane w sposób systemowy i uporządkowany, ponieważ w MSW nie dokonano oszacowania, jakie zasoby ludzkie (w tym wymagane kwalifikacje i odbyte szkolenia) są niezbędne do realizacji zadań związanych z ochroną cyberprzestrzeni. W trakcie kontroli prowadzono prace związane z dokonaniem takiego szacowania.

(dowód: str. 15-25, 30, 55-57, 65-67)

MSW nie prowadziło samodzielnie, ani nie uczestniczyło w organizowanych przez inne podmioty kampaniach informacyjno-edukacyjnych dotyczących bezpieczeństwa w cyberprzestrzeni RP. Ministerstwo nie uczestniczyło również w wypracowaniu założeń tego rodzaju kampanii.

(dowód: str. 17-22)

MSW nie uczestniczyło w inicjatywach społecznych mających na celu realizację zadań zbieżnych z celami *Polityki*.

(dowód: str. 23-24-55-57)

2.5 Wspieranie badań i rozwoju w obszarze ochrony cyberprzestrzeni.

W okresie objętym kontrolą, MSW nie proponowało tematów projektów naukowo-badawczych dotyczących ochrony cyberprzestrzeni RP, ani nie uczestniczyło w opiniowaniu, realizacji lub wdrażaniu takich projektów. W trakcie kontroli trwały wstępne prace mające na celu określenie możliwości realizacji w ww. zakresie projektu we współpracy z Naukową i Akademicką Siecią Komputerową oraz Narodowym Centrum Badań i Rozwoju.

(dowód: str. 17-22, 58-61, 68-73)

Ustalone nieprawidłowości

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

W całym okresie objętym kontrolą, Minister Spraw Wewnętrznych nie realizował, w stosunku do podmiotów podległych lub nadzorowanych obowiązków kontrolnych wymienionych w art. 25 ust. 1 pkt 3 lit. b ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne, w tym, w zakresie sprawdzenia minimalnych zabezpieczeń systemów teleinformatycznych wykorzystywanych przez te jednostki. Stwierdzono również, że w Ministerstwie nie dysponowano wiedzą na temat pełnej liczby i rodzaju systemów teleinformatycznych podlegających kontroli Ministra Spraw Wewnętrznych na podstawie ww. przepisu.

Odpowiedzialność za powstanie opisanych powyżej nieprawidłowości ponoszą osoby zajmujące w okresie objętym kontrolą stanowisko Ministra Spraw Wewnętrznych oraz członkowie Kierownictwa Ministerstwa sprawujący nadzór nad realizacją zadań związanych z ochroną cyberprzestrzeni.

Ocena cząstkowa

Kontrola wykazała, że MSW nie realizowało żadnych zadań związanych z bezpieczeństwem teleinformatycznym skierowanych do użytkowników i administratorów cyberprzestrzeni spoza resortu spraw wewnętrznych. W szczególności Ministerstwo nie podejmowało działań mających na celu wprowadzenie do KPZK procedur reagowania kryzysowego w sytuacjach zagrożeń związanych z cyberprzestrzenią oraz nie uczestniczyło w ćwiczeniach i kampaniach edukacyjnych dotyczących bezpieczeństwa IT. Działania Ministra Spraw Wewnętrznych były ograniczone do własnych sieci i systemów resortowych, natomiast nawet w tym wąskim obszarze nie miały one charakteru systemowego i uporządkowanego. Należy podkreślić, że od momentu utworzenia Ministerstwa nie określono zasad i wymagań bezpieczeństwa informacji przetwarzanych w systemach teleinformatycznych MSW - pomimo upływu prawie półtora roku od powołania zespołu do określenia takich zasad. Nie realizowano również w ogóle

obowiązku kontroli systemów teleinformatycznych wykorzystywanych przez jednostki podległe i nadzorowane, określonego w art. 25 ust. 1 pkt 3 lit. b ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne.

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 Kontroli[17], wnosi o:

1) podjęcie, w uzgodnieniu z Ministrem Administracji i Cyfryzacji, działań mających na celu zdefiniowanie roli i zadań Ministra Spraw Wewnętrznych w ramach budowanego systemu ochrony cyberprzestrzeni RP oraz oszacowanie zasobów Ministerstwa niezbędnych do ich rzetelnej realizacji;

2) bezzwłoczną realizację zadań wynikających z *Polityki*, w szczególności dotyczących oszacowania ryzyka dla systemów teleinformatycznych MSW oraz przekazania Ministrowi Administracji i Cyfryzacji informacji wymaganych na podstawie pkt 5 i 6 tego dokumentu;

3) podjęcie działań w celu realizacji obowiązków kontrolnych wynikających z art. 25 ust. 1 pkt 3 lit. b ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne;

4) zintensyfikowanie działań mających na celu opracowanie i wdrożenie Polityki Bezpieczeństwa Informacji Ministerstwa Spraw Wewnętrznych.

V. Pozostałe informacje i pouczenia

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

Prawo zgłoszenia zastrzeżeń

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

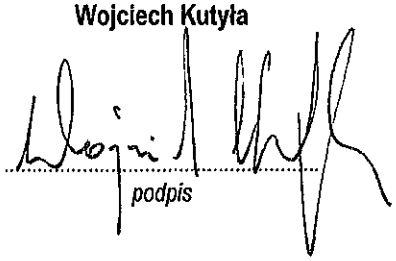
Obowiązek poinformowania NIK o sposobie wykorzystania uwag i wykonania wniosków

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, 24.09.2014 r.

Wiceprezes
Najwyższej Izby Kontroli
Wojciech Kutyła



podpis

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