NAJWYŻSZA IZBA KONTROLI

Departament Porządku i Bezpieczeństwa Wewnętrznego

KPB-4101-002-06/2014
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*

Mariusz Mijewski, główny specjalista kontroli państwowej, upoważnienie do kontroli nr 89662 z dnia 02 czerwca 2014 r.

Adam Zakrzewski, główny specjalista kontroli państwowej, upoważnienie do kontroli nr 92635 z dnia 09.10.2014 r.

Mariusz Perzyna, specjalista kontroli państwowej, upoważnienie do kontroli nr 89663 z dnia 02 czerwca 2014 r.

Dowód: akta kontroli str.: 1-4, tom II str.: 1-2

*Jednostka kontrolowana*

Rządowe Centrum Bezpieczeństwa (zwane dalej RCB)
ul. Aleje Ujazdowskie 5, 00-583 Warszawa

*Kierownik jednostki kontrolowanej*

Antoni Podolski od 2.08.2008 -01.09.2009 r.
Przemysław Guła p.o dyrektora od 22.09.2009 r. do 28.12.2009 r.
Marcin Samsonowicz-Górski od 29.12.2009 r. do 21.12.2010 r.
Marek Komorowski p.o dyrektora od 22.12.2010 r. do 14.06.2012 r.
Marek Komorowski od 15.06.2012 r. do 14.04.2014 r.
Krzysztof Malesa p.o. od 15.04.2014 r. do 28.04.2014 r.
Janusz Skulich od 29.04.2014 r. - nadal

Dowód: akta kontroli str.: 94

# II. Ocena kontrolowanej działalności

**Ocena ogólna**

Kontrola wykazała[1], że Dyrektor Rządowego Centrum Bezpieczeństwa[2] w ramach realizacji zadań wynikających z ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym[3] inicjował i podejmował działania, które należy zdefiniować, jako dobre praktyki związane z ochroną cyberprzestrzeni Rzeczypospolitej Polskiej (cyberprzestrzeni RP). Dotyczyły one w szczególności:

Uzasadnienie oceny ogólnej

- opracowania i zawarcia w załączniku nr 2 do Narodowego Programu Ochrony Infrastruktury Krytycznej ogólnych zasad i rekomendacji dotyczących ochrony teleinformatycznej obiektów infrastruktury krytycznej;
- przygotowania projektu nowelizacji zarządzenia nr 74 Prezes Rady Ministrów[4] dotyczącej m.in. ustanowienia czterech stopni alarmowych, wprowadzanych w razie wystąpienia zagrożeń o charakterze terrorystycznym lub sabotażowym

[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 początku 2008 r. do dnia zakończenia czynności kontrolnych, tj.14 listopada 1014 r.

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

[4] Zarządzenie nr 74 Prezesa Rady Ministrów z dnia 12 października 2011 r. w sprawie wykazu przedsięwzięć i procedur systemu zarzadzania kryzysowego.

dla systemów teleinformatycznych administracji państwowej oraz infrastruktury krytycznej;

– upowszechniania tematyki dotyczącej ochrony teleinformatycznej infrastruktury krytycznej, m.in. w formie specjalnego informatora publikowanego na stronach internetowych RCB.

Ponadto Dyrektor RCB zrealizował zadania wynikające z *Polityki Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej* (zwanej dalej *Polityką*)[5] dotyczące szacowania ryzyk dla systemów teleinformatycznych wykorzystywanych przez RCB oraz powołania w urzędzie pełnomocnika ds. bezpieczeństwa cyberprzestrzeni. Ustalenia kontroli wykazały natomiast, że działania związane z zarządzaniem kryzysowym i ochroną infrastruktury krytycznej są w niewielkim stopniu komplementarne w stosunku do działań mających na celu ochronę cyberprzestrzeni RP. W praktyce, poza zdefiniowanymi powyżej dobrymi praktykami, ww. procesy koordynowane odpowiednio przez RCB oraz Ministerstwo Administracji i Cyfryzacji (MAiC) były rozłączne, niespójne i nie uzupełniały się wzajemnie. W szczególności, nie zapewniono porównywalności wyników szacowania ryzyka (prowadzonego na podstawie ustawy o zarządzaniu kryzysowym oraz *Polityki)* dla teleinformatycznej infrastruktury państwa oraz nie aktualizowano i nie dostosowywano na bieżąco kluczowych dokumentów i procedur z zakresu zarządzania kryzysowego, w celu zapewnienia możliwości ich wykorzystania w ramach budowanego systemu ochrony cyberprzestrzeni RP. Powyższe wynikało m.in. z faktu, że wdrażanie systemu zarządzania kryzysowego zostało rozpoczęte znacznie wcześniej, niż działania systemowe mające na celu ochronę cyberprzestrzeni, co powoduje, że oba te procesy znajdują się w różnych stadiach zawansowania. Należy również podkreślić, że RCB nie otrzymywało żadnych wskazówek, wytycznych, itp. ze strony Ministra Administracji i Cyfryzacji[6], który odpowiada za koordynację zadań związanych z ochroną cyberprzestrzeni RP i powinien inicjować działania mające na celu zapewnienie spójności i komplementarności wszystkich procesów związanych z ochroną teleinformatycznej infrastruktury krytycznej państwa. W trakcie trwania kontroli NIK, Dyrektor RCB wystąpił z inicjatywą działań zmierzających do zapewnienia spójności i komplementarności procesów zarządzania kryzysowego oraz ochrony cyberprzestrzeni, przedstawiając propozycje tematów prac *Zespołu zadaniowego do spraw bezpieczeństwa cyberprzestrzeni Rzeczypospolitej Polskiej* dotyczące: identyfikacji systemów infrastruktury krytycznej związanych z zachowaniem bezpieczeństwa w cyberprzestrzeni oraz ujednolicenia metodyk szacowania ryzyka.

# III. Opis ustalonego stanu faktycznego

## 1. Zasoby do realizacji zadań związanych z ochroną cyberprzestrzeni RP.

Opis stanu faktycznego

RCB jest państwową jednostką budżetową podlegająca Prezesowi Rady Ministrów, zapewniającą obsługę Rady Ministrów, Prezesa Rady Ministrów, Rządowego Zespołu Zarządzania Kryzysowego i ministra właściwego do spraw wewnętrznych w sprawach zarządzania kryzysowego oraz pełniącą funkcję krajowego centrum zarządzania kryzysowego. Organizacja i tryb działania RCB zostały określone na podstawie rozporządzenia Prezesa Rady Ministrów z dnia 11 kwietnia 2011 r.[7].

[5] Przyjętej uchwałą Rady Ministrów z dnia 25 czerwca 2013 r.
[6] Wcześniej – Ministra Spraw Wewnętrznych i Administracji.
[7] Dz. U. z 2011 r. Nr 86, poz. 471.

W ramach struktury RCB można wyróżnić trzy komórki organizacyjne uczestniczące w realizacji zadań związanych z ochroną cyberprzestrzeni RP:

1. Zespół Informatyki i Łączności Wydziału Administracyjno-Finansowego - odpowiadający za utrzymanie ciągłości funkcjonowania oraz bezpieczeństwo jawnych i niejawnych systemów teleinformatycznych RCB.
2. Wydział Ochrony Infrastruktury Krytycznej realizujący zadania obejmujące w szczególności: identyfikację obiektów, urządzeń, instalacji i usług wchodzących w skład infrastruktury krytycznej RP, prowadzenie wykazu infrastruktury krytycznej, definiowanie zasad ochrony infrastruktury krytycznej (w tym ochrony teleinformatycznej) oraz opiniowanie planów ochrony infrastruktury krytycznej. Pracownicy Wydziału uczestniczyli w ćwiczeniach dotyczących bezpieczeństwa cyberprzestrzeni (opisanych na str. 7 wystąpienia) oraz biorą udział w przygotowywaniu publikowanego przez RCB kwartalnika *CIIP focus* na temat ochrony teleinformatycznej infrastruktury krytycznej (opisano na str. 8 wystąpienia).
3. Wydział Planowania odpowiadający za przygotowanie i aktualizację następujących dokumentów i regulacji z zakresu zarządzania kryzysowego: Raportu o zagrożeniach bezpieczeństwa narodowego, Krajowego Planu Zarządzania Kryzysowego, zarządzenia nr 74 Prezesa Rady Ministrów w sprawie wykazu przedsięwzięć i procedur systemu zarządzania kryzysowego.

W przypadku komórek organizacyjnych RCB wymienionych w pkt 2 i 3 działania związane z ochroną cyberprzestrzeni (teleinformatycznej infrastruktury krytycznej) realizowane były w ramach ogólnych zadań tych Wydziałów związanych z zarządzaniem kryzysowym i ochroną krajowej infrastruktury krytycznej.

Dowód: akta kontroli str.: 135-136

Ponadto, zgodnie z zapisami *Polityki*, w RCB wyznaczono Pełnomocnika ds. bezpieczeństwa cyberprzestrzeni, która to funkcja została powierzona pracownikowi Zespołu Informatyki i Łączności Wydziału Administracyjno-Finansowego. Pełnomocnik zrealizował zadania wynikające z *Polityki* dotyczące szacowania ryzyka dla systemów teleinformatycznych RCB oraz oszacowania (i przekazania do Ministra Administracji i Cyfryzacji) osiągniętych i sugerowanych wskaźników realizacji zadań wynikających z *Polityki*. Pełnomocnik prowadził także prace związane z przyjęciem i wdrożeniem *Globalnej Polityki Bezpieczeństwa* RCB.

Dowód: akta kontroli str.: 21-22, 135-136

W 2012 i w 2013 r. wydatki RCB na zakup sprzętu i oprogramowania komputerowego wykorzystywanych do zabezpieczenia systemów teleinformatycznych urzędu wyniosły odpowiednio 262,9 tys. zł i 134,4 tys. zł. W 2014 r. planowane jest wydatkowanie na ww. zakupy kwoty 170 tys. zł[8]. Stwierdzono natomiast, że wg stanu na dzień 27 lipca 2014 r. w RCB nie przeprowadzono kompleksowego szacowania wszystkich zasobów oraz wydatków związanych z ochroną cyberprzestrzeni RP. Przedmiotowe wydatki nie były odrębnie ewidencjonowane, ani wydzielane w ramach planu finansowego urzędu. W związku z powyższym 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.

[8] Na koniec III kwartału 2014 r. wydatkowano kwotę 133, 4 tys. zł.

Dyrektor RCB wyjaśnił, że nie zrealizowano ww. zadań, ponieważ w *Polityce* nie określono w sposób precyzyjny zasad szacowania, ewidencjonowania oraz trybu przekazywania informacji o poniesionych i planowanych wydatkach związanych z ochroną cyberprzestrzeni. Nie otrzymano również w ww. zakresie żadnych wytycznych z MAiC. Poinformował, że w chwili obecnej w RCB prowadzone są prace mające na celu oszacowanie wydatków poniesionych na realizację dotychczasowych zadań związanych z ochroną cyberprzestrzeni RP. Po zakończeniu tych prac, stosowne informacje zostaną przekazane do MAiC. Wskazał także, że RCB niezwłocznie po opracowaniu dokumentów planistycznych na 2015 r., przekaże do MAiC dane dotyczące kosztów realizacji zadań dotyczących ochrony cyberprzestrzeni planowanych na rok następny.

Dowód: akta kontroli str.: 10-11,121-122,135

Ustalono, iż powyższy obowiązek Dyrektor RCB zrealizował w trakcie trwania kontroli NIK (w dniu 21 października 2014 r.). W przesłanym do MAiC zestawieniu przekazano kwoty wydatkowane przez RCB na zadania związane z zapewnieniem bezpieczeństwa informacji i ochroną cyberprzestrzeni w latach 2012-2014 (wg stanu na koniec III kwartału 2014 r.) oraz planowane wydatki na powyższe zadania w 2015 r.

Dowód: akta kontroli tom II str.: 9-10, 29

Ustalone nieprawidłowości

W działalności kontrolowanej jednostki w przedstawionym wyżej zakresie nie stwierdzono nieprawidłowości.

Uwagi dotyczące badanej działalności

NIK zwraca uwagę, że zadania dotyczące ochrony cyberprzestrzeni są realizowane przez komórki organizacyjne i pracowników RCB równolegle z innymi obowiązkami służbowymi dotyczącymi zarządzania kryzysowego, w związku z czym szacowanie wydatków na ich realizację może być nieprecyzyjne i obarczone znacznym błędem. W związku z powyższym, w celu rzetelnego wykonywania obowiązków określonych w pkt 5 *Polityki*, zasadne wydaje się wystąpienie do Ministra Administracji i Cyfryzacji o przedstawienie wytycznych w zakresie ewidencjonowania i szacowania zasobów oraz wydatków związanych z ochroną cyberprzestrzeni, a także trybu przekazywania tych informacji do MAiC.

**Ocena cząstkowa**

Kontrola wykazała, że Dyrektor RCB wyznaczył zasoby odpowiedzialne za ochronę teleinformatyczną wewnętrznych systemów urzędu oraz zgodnie z zapisami *Polityki* powołał w RCB Pełnomocnika ds. bezpieczeństwa cyberprzestrzeni. Pozostałe zadania związane z ochroną cyberprzestrzeni były realizowane przez komórki organizacyjne[9] i pracowników RCB równolegle z innymi obowiązkami służbowymi dotyczącymi zarządzania kryzysowego.

## 2. Opracowanie i wdrożenie Polityki Ochrony Cyberprzestrzeni RP.

Opis stanu faktycznego

Kontrola wykazała, że RCB nie uczestniczyło w pracach nad przygotowaniem Polityki Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej oraz nie było uwzględnione w konsultacjach międzyresortowych projektu przedmiotowej regulacji. Dyrektor RCB poinformował, że nie posiada informacji o podmiocie decydującym oraz o przyczynach nieuwzględnienia RCB w procesie konsultacji i uzgodnień Polityki.

Dowód: akta kontroli str.: 10

***Realizacja zadań RCB wynikających z Polityki ochrony cyberprzestrzeni RP.***

W ramach realizacji obowiązków wynikających z *Polityki,* wg stanu na dzień 14 listopada 2014 r., w RCB realizowano następujące zadania:

[9] Wydział Ochrony Infrastruktury Krytycznej oraz Wydział Planowania.

- zgodnie z zapisami pkt 3.1. *Polityki* przeprowadzono szacowanie ryzyka związanego z funkcjonowaniem cyberprzestrzeni w zakresie systemów teleinformatycznych wykorzystywanych przez RCB. Szacowanie ryzyka zostało zrealizowane w oparciu o metodykę otrzymaną w dniu 18 lutego 2014 r. z MAiC i obejmowało krytyczne zasoby teleinformatyczne urzędu wybrane przez Pełnomocnika ds. bezpieczeństwa cyberprzestrzeni, pracowników Zespołu Informatyki i Łączności oraz pionu ochrony RCB. Wyniki szacowania ryzyka zostały terminowo przekazane do MAiC. W piśmie przekazującym wyniki, RCB wskazywało na liczne braki koordynowanego przez MAiC procesu, tj. w szczególności opóźnienie w przekazaniu metodyki szacowania ryzyka oraz brak przeszkolenia pełnomocników ds. ochrony cyberprzestrzeni. Ustalono, że RCB nie uczestniczyło i nie współpracowało w procesie przygotowania metodyki, która była wykorzystana w ramach procesu szacowania ryzyk realizowanego na podstawie pkt 3.1. *Polityki*;

  Dowód: akta kontroli str.: 12-13, 95-131

- zgodnie z pkt 3.4.2. *Polityki* w RCB prowadzone były prace mające na celu wdrożenie kompleksowego systemu zarządzania bezpieczeństwem informacji i ujednolicenie obowiązujących w tym obszarze w RCB regulacji[10]. Zasoby informacyjne RCB zostały zidentyfikowane, zredagowano strukturę przedmiotowego dokumentu oraz podzielono zadania do opracowania poszczególnych części dokumentu pomiędzy pracowników Centrum. Osoby odpowiedzialne za opracowanie materiału zapoznały się ze standardami i dobrymi praktykami w zakresie konstruowania polityki bezpieczeństwa informacji. Ponadto dokonały analizy tego rodzaju dokumentów wdrożonych w innych instytucjach publicznych.

  Z wyjaśnień Dyrektora RCB wynika, iż Rządowe Centrum Bezpieczeństwa planuje opracowanie dokumentu *Globalna Polityka Bezpieczeństwa* do końca bieżącego roku, zaś jego wdrożenie w I półroczu 2015 r.

  Dowód: akta kontroli str.:11-12, 134-135, tom II str.:10

- na podstawie pkt 3.4.3. *Polityki* w RCB wyznaczony został Pełnomocnik ds. bezpieczeństwa cyberprzestrzeni;

  Dowód: akta kontroli str.: 21-22, 135-136

- zgodnie z pkt 6. *Polityki,* w dniu 25 czerwca 2014 r. przesłano do MAiC informację na temat przyjętych i osiągniętych przez RCB wskaźników realizacji zadań wynikających z wdrażania tego dokumentu. W dokumencie pt. *Ocena stopnia realizacji Polityki ochrony cyberprzestrzeni Rzeczypospolitej Polskiej w Rządowym Centrum Bezpieczeństwa* zawarto następujące wskaźniki dotyczące zadań RCB związanych z ochroną wewnętrznych zasobów informatycznych urzędu: przeprowadzenie analizy ryzyka dla systemów RCB działających w cyberprzestrzeni RP, reagowanie na incydenty oraz współpraca z CERT, wdrażanie mechanizmów ochrony sprzętowej i programowej, wdrażanie mechanizmów proceduralnych oraz podnoszenie kwalifikacji zawodowych pracowników RCB. Analiza dotyczyła okresu od 25 czerwca 2013 r do 25 czerwca 2014 r.

  Dowód: akta kontroli str.: 10,121-122,135

[10] Tj. „Plan ochrony informacji niejawnych oraz innych zasobów w Rządowym Centrum Bezpieczeństwa"., „Polityka Bezpieczeństwa Danych Osobowych w RCB", „Decyzja Dyrektora Rządowego Centrum Bezpieczeństwa w sprawie funkcjonowania systemu teleinformatycznego do Elektronicznego Zarządzania Dokumentacją oraz organizacji czynności kancelaryjnych w Rządowym Centrum Bezpieczeństwa" (1/2013).

Wg stanu na dzień 14 listopada 2014 w RCB zrealizowano również zadania wymienione w pkt 5. *Polityki* dotyczące przekazania Ministrowi Administracji i Cyfryzacji informacji na temat wykonanych dotychczas zadań związanych z ochroną cyberprzestrzeni oraz wydatków poniesionych i planowanych na ich realizację (opisano szczegółowo w pkt III.1. wystąpienia pokontrolnego).

***Ćwiczenia, szkolenia i działalność edukacyjna.***

Wg stanu na dzień 21 października 2014 r. RCB nie organizowało ćwiczeń z zakresu bezpieczeństwa cyberprzestrzeni, uczestniczyło natomiast w następujących ćwiczeniach dotyczących ww. obszaru:

- Cyber-Exe Polska 2012, Cyber-Exe Polska 2013 oraz Cyber-EXE Polska 2014 - ćwiczenia zostały zorganizowane przez Fundację Bezpieczna Cyberprzestrzeń, a RCB objęło ww. imprezę patronatem oraz wsparło merytoryczne organizatora i uczestników;
- Cyber Europe 2012 oraz Cyber Europe 2014 - ćwiczenia zostały zorganizowane prze Europejską Agencję ds. Bezpieczeństwa Sieci i Informacji. W 2012 r. RCB uczestniczyło w programie dla obserwatorów skierowanym do państw i organizacji nieuczestniczących aktywnie w ćwiczeniu, a w 2014 r. koordynowało udział strony polskiej w fazie technicznej ćwiczeń i moderowało jej przebieg. RCB nie planuje udziału w kolejnych fazach ćwiczenia Cyber Europe 2014;
- NATO CMX 2012 - ćwiczenia z zakresu zarządzania kryzysowego zostały zorganizowane przez NATO i zawierały wątki związane z ochroną teleinformatyczną. RCB pełniło rolę krajowego koordynatora ćwiczenia. Rządowe Centrum Bezpieczeństwa bierze udział w pracach zespołu planistycznego ćwiczenia NATO CMX 2015 na poziomie międzynarodowym. Na poziomie krajowym koordynuje udział polskich podmiotów w przedmiotowych ćwiczeniach;
- Cyber 2013 – ćwiczenia zostały zorganizowane przez Europejską Komórkę Koordynacji Kryzysowej ds. Lotnictwa we współpracy z Europejską Organizacją ds. Bezpieczeństwa Żeglugi Powietrznej. Wydział Operacyjny RCB pełnił w tym ćwiczeniu rolę obserwatora.

Dowód: akta kontroli str.: 13-19, tom II str.: 10

Pracownicy RCB, w momencie podjęcia zatrudnienia w tej instytucji, uczestniczyli we wstępnym szkoleniu, w ramach którego uzyskiwali podstawową wiedzę o zasadach bezpieczeństwa w korzystaniu z urządzeń i systemów teleinformatycznych. Ponadto w latach 2012 -2014 pracownicy RCB wzięli udział w następujących specjalistycznych szkoleniach z zakresu bezpieczeństwa IT:

- w roku 2012: szkolenie administratorów i inspektorów bezpieczeństwa teleinformatycznego (2 pracowników), konfiguracja i dostosowanie ArcGIS Serwer (1 pracownik), spotkanie architektów Microsoft (1 pracownik), wykorzystanie podpisu elektronicznego w systemie Edicta (1 pracownik);
- w roku 2013: analiza ryzyka dla informacji niejawnych i ochrony informacji niejawnych (2 pracowników), spotkanie architektów Microsoft (2 pracowników), praktyczny kurs informatyki śledczej – poziom specjalisty (1 pracownik), podstawy zarządzania wymaganiami REQB (1 pracownik), Seminar on Transatlantic Civil Security – ochrona ludności w cyberprzestrzeni: prawo, technologia, polityka (1 pracownik);

– w roku 2014 (do 30 lipca): Seminar on Transnational Civil Security – zagrożenia cyberprzestrzeni (2 pracowników).

Dowód: akta kontroli str.:19, 21-23

W okresie objętym kontrolą, RCB nie opracowało samodzielnie ani nie uczestniczyło w opracowaniu założeń kampanii informacyjno-edukacyjnych prowadzonych przez inne instytucje, dotyczących ochrony cyberprzestrzeni RP. Ustalono natomiast, że RCB realizowało następujące działania edukacyjne mające na celu upowszechnianie tematyki związanej z zagrożeniami występującymi w cyberprzestrzeni oraz ochroną teleinformatyczną infrastruktury krytycznej:

– od 2012 r na stronie internetowej RCB publikowane jest kwartalne opracowanie *CIIP focus – informator o ochronie teleinformatycznej*, w którym umieszczane są aktualności z obszaru cyberbezpieczeństwa, artykuły dotyczące zagadnień ochrony teleinformatycznej oraz relacje i wywiady związane z zagadnieniami bezpieczeństwa cyberprzestrzeni;

– opracowano załącznik nr 2 do Narodowego Programu Ochrony Infrastruktury Krytycznej, w którym zamieszczono standardy i dobre praktyki służące zapewnieniu sprawnego funkcjonowania infrastruktury krytycznej (w tym także w obszarze cyberprzestrzeni – ochrona teleinformatyczna);

– zorganizowano wspólnie z PSE S.A. konferencję pn. *Ochrona Teleinformatyczna Infrastruktury Krytycznej* – skierowaną do operatorów infrastruktury krytycznej oraz podmiotów sektora elektroenergetycznego.

Dowód: akta kontroli str.: 19-20, tom II str.: 10

***Wspieranie badań i rozwoju w obszarze ochrony cyberprzestrzeni.***

W okresie objętym kontrolą RCB nie składało propozycji tematów projektów naukowo-badawczych dotyczących ochrony cyberprzestrzeni. Opiniowało jedynie projekt realizowany przez Wojskowy Instytut Łączności (WIŁ) ze środków Narodowego Centrum Badań i Rozwoju pod tytułem *System ewaluacji zagrożeń bezpieczeństwa cyberprzestrzeni RP na potrzeby systemu zarzadzania bezpieczeństwem narodowym Rzeczypospolitej Polskiej*[11]. Przedstawiciele WIŁ w dniu 5 lutego 2014 r. przedstawili RCB założenia projektu. Ze względu na fakt, że w ramach prowadzonych prac nie przewiduje się elementów związanych z ochroną teleinformatyczną poszczególnych obiektów infrastruktury krytycznej, RCB nie widziało możliwości udziału w ww. projekcie.

Dowód: akta kontroli str.: 20, tom II str.: 10

Ustalone nieprawidłowości

W działalności kontrolowanej jednostki w przedstawionym wyżej zakresie nie stwierdzono nieprawidłowości.

Uwagi dotyczące badanej działalności

NIK zwraca uwagę, że opracowane na podstawie pkt 6 *Polityki* wskaźniki realizacji zadań RCB, wynikających z wdrażania tego dokumentu, odnoszą się tylko do działań związanych z ochroną wewnętrznych zasobów informatycznych urzędu i nie uwzględniają kluczowych zadań tego podmiotu w zakresie ochrony krajowej teleinformatycznej infrastruktury krytycznej. Powyższe wskazuje na istotny problem związany ze zdefiniowaniem faktycznej roli RCB w budowanym obecnie systemie ochrony cyberprzestrzeni RP. Zdaniem NIK, zasadne jest więc podjęcie efektywnego dialogu między RCB a MAiC w celu określenia zasad współpracy w ramach ochrony cyberprzestrzeni i zarządzania kryzysowego oraz zadań RCB w tym zakresie.

[11] Temat nr 11 w konkursie 4/2013.

Ocena cząstkowa

Kontrola wykazała, że w RCB zrealizowano zadania nałożone na ten podmiot na podstawie *Polityki*, tj. przeprowadzono szacowanie ryzyka odnośnie zasobów teleinformatycznych urzędu, wyznaczono Pełnomocnika ds. bezpieczeństwa cyberprzestrzeni oraz określono i przekazano do MAiC wskaźniki realizacji zadań RCB wynikających z wdrażania tego dokumentu. W trakcie kontroli NIK, w RCB zrealizowano również zadania wymienione w pkt 5. *Polityki* dotyczące przekazania Ministrowi Administracji i Cyfryzacji informacji na temat wykonanych dotychczas zadań związanych z ochroną cyberprzestrzeni oraz wydatków poniesionych i planowanych na ich realizację (opisano szczegółowo w pkt III.1. wystąpienia pokontrolnego).

W działaniach RCB zdefiniowano również dobre praktyki polegające na podejmowaniu samodzielnych inicjatyw w zakresie działań edukacyjnych dotyczących ochrony cyberprzestrzeni. Podjęte działania dotyczyły m.in. publikowania informatora poświęconego zagadnieniom ochrony teleinformatycznej infrastruktury krytycznej.

### 3. Realizacja zadań RCB związanych z ochroną cyberprzestrzeni w obszarze zarządzania kryzysowego.

***Raport o zagrożeniach bezpieczeństwa narodowego.***

Opis stanu faktycznego

Raport o zagrożeniach bezpieczeństwa narodowego jest podstawą systemu zarządzania kryzysowego, ponieważ zgodnie z art. 5a ustawy o zarządzaniu kryzysowym, w dokumencie tym zdefiniowane są najważniejsze zagrożenia dla infrastruktury państwa oraz rekomendacje działań wymaganych w celu ich ograniczenia. Raport o zagrożeniach bezpieczeństwa narodowego (zwany dalej *Raportem*) został przyjęty uchwałą Rady Ministrów z dnia 24 czerwca 2011 r. oraz znowelizowany na podstawie uchwały z dnia 12 lipca 2013 r.

W wyniku analizy przygotowanych przez RCB Raportów z 2011 i 2013 r. stwierdzono, że w ww. dokumentach zawarto opis zagrożeń związanych z cyberprzestrzenią, który został opracowany na postawie raportu cząstkowego Agencji Bezpieczeństwa Wewnętrznego w obszarze zagrożeń spowodowanych intencjonalną działalnością człowieka. W Raportach określono ogólne cele strategiczne oraz propozycje przedsięwzięć i zadań w zakresie poprawy bezpieczeństwa cyberprzestrzeni. W sposób ramowy określono priorytety w reagowaniu na zagrożenia cyberprzestrzeni oraz siły i środki niezbędne do osiągnięcia celów strategicznych.

Dowód akta kontroli str.: 56 - 63; 67-72; 284

Na etapie sporządzania Raportów o zagrożeniach bezpieczeństwa narodowego przyjętych w 2011 i 2013 r. zagrożenia dotyczące cyberprzestrzeni zostały wskazane w raportach cząstkowych następujących instytucji:

- przedstawione jako zagrożenie w raportach: Ministra Administracji i Cyfryzacji, Ministra Edukacji Narodowej, Ministra Zdrowia (NFZ), Szefa Agencji Bezpieczeństwa Wewnętrznego oraz Wojewody Warmińsko-Mazurskiego;
- zdefiniowane jako możliwy scenariusz zagrożenia w raportach: Ministra Obrony Narodowej, Ministra Spraw Wewnętrznych, Ministra Rolnictwa i Rozwoju Wsi Ministra Nauki i Szkolnictwa Wyższego, Ministra Sportu i Turystyki, Szefa Agencji Wywiadu;
- wskazane jako możliwa przyczyna wystąpienia zagrożenia w raportach cząstkowych: Ministra Finansów, Ministra Transportu, Budownictwa i Gospodarki Morskiej, Ministra Sprawiedliwości oraz Wojewodów: Dolnośląskiego, Łódzkiego, Małopolskiego, Opolskiego, Śląskiego,

Świętokrzyskiego i Wielkopolskiego.

Ustalono, że na etapie sporządzania Raportów z 2011 i 2013 r., Dyrektor RCB nie korzystał z przysługujących mu uprawnień i nie zwracał się do wykonawców raportów cząstkowych z zastrzeżeniami lub uwagami dotyczącymi uzupełnienia ich treści o problematykę dotyczącą zagrożeń występujących w cyberprzestrzeni, ani o uszczegółowienie informacji dotyczących tych zagrożeń. Nie występował również do wykonawców raportów cząstkowych o ich wcześniejszą aktualizację. Z wyjaśnień Dyrektora RCB wynika, że w przypadku raportów zawierających zagrożenia cyberprzestrzeni, nie zaistniała taka potrzeba.

Dowód akta kontroli: str.: 75 – 76

Raporty o zagrożeniach bezpieczeństwa narodowego (cząstkowe i zbiorczy) zostały przygotowane w oparciu o metodykę, której autorem jest RCB.

Kontrola wykazała, że RCB nie podejmowało działań mających na celu zapewnienie porównywalności i komplementarności wyników szacowania ryzyka realizowanego na podstawie ustawy o zarządzaniu kryzysowym (w ramach Raportów) z wynikami szacowania ryzyka realizowanego na podstawie Polityki. Nie była również prowadzona współpraca pomiędzy RCB a MAiC oraz Zespołem CERT.GOV.PL[12] mająca na celu wytworzenie jednolitej metodyki szacowania ryzyk związanych ze zdarzeniami występującymi w cyberprzestrzeni.

Dyrektor RCB wyjaśnił m.in. że *(...) trudno jest mówić o porównywalności i komplementarności wyników szacowania ryzyka realizowanego na podstawie ustawy o zarzadzaniu kryzysowym oraz na podstawie Polityki. Widoczna jest, zdaniem RCB, różnica w zakresie genezy dotyczącej skali, tj. obszary przedmiotowe obu analiz są odległe, operują na innej skali zagrożeń, mają inne cele i stosowane są inne metody*. Wskazał także, że zdaniem RCB nie powinna być prowadzona współpraca z MAiC i Zespołem CERT.GOV.PL w celu wytworzenie jednolitej metodyki szacowania ryzyk związanych ze zdarzeniami występującymi w cyberprzestrzeni ponieważ *(...) zarzadzanie kryzysowe bazuje na analizie w skali makro, natomiast na potrzeby realizacji Polityki wdrażana jest metodyka dotycząca szczegółowej analizy zagrożeń dla konkretnych systemów teleinformatycznych.*

Dowód: akta kontroli str.: 13

W trakcie kontroli NIK, Dyrektor RCB przedstawił propozycję tematów prac Zespołu zadaniowego do spraw bezpieczeństwa cyberprzestrzeni Rzeczypospolitej Polskiej. Wśród zaproponowanej problematyki zawarto propozycję podjęcia działań w celu doprowadzenia do sytuacji, w której wyniki oceny ryzyka sporządzanej na potrzeby Polityk Ochrony Cyberprzestrzeni RP były możliwe do wykorzystania w ramach oceny ryzyka sporządzanej na potrzeby Raportu o zagrożeniach bezpieczeństwa narodowego.

Dowód: akta kontroli tom II str.: 4

***Krajowy Plan Zarządzania Kryzysowego.***

Krajowy Plan Zarządzania Kryzysowego (zwany dalej *KPZK* lub *Planem*) został przyjęty przez Radę Ministrów 6 marca 2012 r. oraz znowelizowany na podstawie uchwały z 23 lipca 2013 roku. Dokument został sporządzony przez RCB, we współpracy z ministerstwami, urzędami centralnymi i województwami.

Dowód akta kontroli str.: 284

KPZK z 2012 r. w części głównej nie uwzględniał zagrożeń związanych ze zdarzeniami występującymi w cyberprzestrzeni.

---

[12] Rządowy Zespół Reagowania na Incydenty Komputerowe.

W części I zaktualizowanego Planu z 2013 r. 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[13]. 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, wynikającą z kierowania działami administracji rządowej informatyzacja i łączność oraz z zapisów *Polityki*. Zagadnienia związane z zagrożeniami występującymi w cyberprzestrzeni zostały uwzględnione w KPZK tylko w kontekście obowiązków ABW w zakresie monitorowania zagrożeń teleinformatycznych i terrorystycznych (część II Planu). Propozycja uzupełniania KPZK o zagrożenia występujące w cyberprzestrzeni została zgłoszona przez Biuro Bezpieczeństwa Narodowego w trakcie międzyresortowej konferencji uzgodnieniowej poświęconej aktualizacji Planu, która odbyła się w dniu 31 stycznia 2013 r.

Dowód akta kontroli str.: 211, 284

Dyrektor RCB wyjaśnił, że na etapie opracowywania KPZK brakowało przyjętej Polityki Ochrony Cyberprzestrzeni RP, pozwalającej zdefiniować ww. zagadnienia. Zgodnie z postanowieniami konferencji uzgodnieniowej dotyczącej aktualizacji KPZK, przedmiotowy dokument miał zostać uzupełniony o powyższe informacje po przyjęciu Polityki Ochrony Cyberprzestrzeni RP przy kolejnej jego aktualizacji.

Dowód akta kontroli str.: 76

Ustalono, iż w trakcie kontroli NIK, w dniu 25 lipca 2014 roku RCB przekazało[14] ministrom, kierownikom urzędów centralnych i wojewodom projekt aktualizacji KPZK. Zawierał on propozycję zmian zapisów w siatce bezpieczeństwa dotyczącej *zadań i obowiązków uczestników zarządzania kryzysowego*. W projekcie dodano m.in. zagrożenia w cyberprzestrzeni oraz zagrożenia systemów telekomunikacyjnych (awarie łączności). Aktualnie (stan na dzień 21 października 2014 r.) w RCB twa proces analizy i doprecyzowywania otrzymanych uwag[15] do przedmiotowego dokumentu[16].

Dowód: akta kontroli str.: 143-144 ,218-231, 265 tom II str.: 10-11

***Narodowy Program Ochrony Infrastruktury Krytycznej oraz plany ochrony infrastruktury krytycznej.***

Narodowy Program Ochrony Infrastruktury Krytycznej (NPOIK) został przyjęty przez Radę Ministrów 26 marca 2013 roku. W Załączniku nr 2 do ww. dokumentu zawarto odrębny rozdział zawierający wskazówki, rekomendacje i dobre praktyki dotyczące ochrony teleinformatycznej obiektów infrastruktury krytycznej. Zakres tematyczny ww. dokumentu obejmuje przykłady cyberataków na infrastrukturę krytyczną oraz zasady ochrony teleinformatycznej infrastruktury krytycznej dotyczące w szczególności: planów awaryjnych, kontroli dostępu, ochrony stacji roboczych, bezpieczeństwa sieci bezprzewodowych, monitoringu zagrożeń, reakcji na incydenty i ich obsługi, wykaz funkcjonujących zespołów CERT.

Dowód akta kontroli str.: 284

Poza załącznikiem nr 2 do NPOIK, RCB nie wydawało rekomendacji lub wytycznych dotyczących bezpieczeństwa systemów teleinformatycznych, które mogłyby zostać wykorzystane przez operatorów infrastruktury krytycznej, np. w celu opracowania planów ochrony infrastruktury krytycznej.

---

[13] Zapobieganie, przygotowanie, reagowanie, odbudowa.
[14] Za pismem nr WP.4160.1.3.2014.TJ
[15] Uwagi do ww. projektu w obszarze cyberprzestrzeni zgłosiły następujące instytucje: MNiSzW, MON, MS, MRiRW, MSW,MAiC ABW, Śląski UW.
[16] Pismo nr WP.4160.1.3.2014/AS z dnia 17.10.2014 r.

Dyrektor RCB wyjaśnił, że nie wydawano tego typu rekomendacji, ponieważ głównym założeniem NPOIK jest oparcie systemu ochrony infrastruktury krytycznej o zasady proporcjonalności i działań opartych na ocenie ryzyka. *(...) Przygotowane dobre praktyki i rekomendacje nie są obowiązkowe. Każdy z operatorów infrastruktury krytycznej po przeprowadzeniu analizy ryzyka i określeniu swoich słabych punktów może skorzystać z dobrych rekomendacji i praktyk, które mają za zadanie obniżenie ryzyka do poziomu akceptowalnego przez operatora. (...).* Wskazał również, że rekomendacje i wnioski z ćwiczeń dotyczących bezpieczeństwa IT (np. Cyber-Exe) są dostępne w Internecie. Ponadto RCB wydawało pojedyncze opinie (po prośbach operatorów infrastruktury krytycznej) dotyczące np. wdrażania konkretnych klas systemów w obiektach IK.

Dowód akta kontroli str.: 5-20, 140-148

W Załączniku nr 3 do NPOIK określono kryteria pozwalające wyodrębnić obiekty, instalacje, urządzenia i usługi wchodzące w skład systemów infrastruktury krytycznej[17]. Kryteria oraz jednolity wykaz infrastruktury krytycznej opracowane zostały i są aktualizowane w RCB we współpracy z ministrami i kierownikami urzędów centralnych.

Obecnie obowiązujący jednolity wykaz obiektów, instalacji, urządzeń i usług wchodzących w skład infrastruktury krytycznej[18], został sporządzony i podpisany przez Dyrektora RCB 14 lipca 2014 r. Zawiera on 689 pozycji podzielonych na 11 systemów infrastruktury krytycznej[19]. Systemy teleinformatyczne[20] wchodzące w skład krajowej infrastruktury krytycznej zawarte są w szczególności w pozycjach: Systemy łączności, Systemy sieci teleinformatycznych oraz Systemy zapewniające ciągłość działania administracji publicznej.

Z wyjaśnień udzielonych przez Dyrektora RCB wynika natomiast, że przy obecnie obowiązujących kryteriach konstruowania wykazu infrastruktury krytycznej nie ma możliwości określenia pełnej liczby, nazw i rodzaju wszystkich systemów teleinformatycznych (w rozumieniu ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne) funkcjonujących w ramach obiektów umieszczonych w Jednolitym Wykazie Infrastruktury Krytycznej. Kryteria nie przewidują bowiem wyłaniania systemów teleinformatycznych funkcjonujących w ramach obiektów IK, jako odrębnej infrastruktury krytycznej. Dyrektor RCB wskazał, że identyfikacja systemów teleinformatycznych może nastąpić dopiero na etapie uzgadniania planów ochrony dla poszczególnych obiektów infrastruktury krytycznej: *Tego typu systemy powinny być wyszczególnione i opisane w Planach Ochrony Infrastruktury Krytycznej*[21] *w części dotyczącej ochrony teleinformatycznej infrastruktury krytycznej.*

Dyrektor RCB poinformował, że w trakcie opracowywania projektu *Kryteriów pozwalających wyodrębnić obiekty, instalacje, urządzenia i usługi wchodzące w skład systemów infrastruktury krytycznej* oraz po przyjęciu przez Radę Ministrów Narodowego Programu Ochrony Infrastruktury Krytycznej ministrowie oraz kierownicy urzędów centralnych nie zgłaszali do RCB żadnych uwag i propozycji mających na celu wykorzystanie danych zbieranych w związku z tworzeniem wykazu infrastruktury krytycznej na potrzeby działań związanych z ochroną

---

[17] Dokument zawierający informacje niejawne o klauzuli ZASTRZEŻONE,

[18] Dokument zawierający informacje niejawne o klauzuli TAJNE.

[19] Zgodnie z art. 3 ust 2 ustawy o zarządzaniu kryzysowym.

[20] Na podstawie art. 3 pkt 3 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2013 r., poz. 235 ze zm.), *system teleinformatyczny* oznacza zespół współpracujących ze sobą urządzeń informatycznych i oprogramowania zapewniający przetwarzanie, przechowywanie, a także wysyłanie i odbieranie danych przez sieci telekomunikacyjne za pomocą właściwego dla danego rodzaju sieci telekomunikacyjnego urządzenia końcowego.

[21] Tworzonych na podstawie art. 6 ust. 5 ustawy o zarządzaniu kryzysowym.

cyberprzestrzeni (np. poprzez zmianę kryteriów identyfikacji infrastruktury krytycznej, która pozwoliłaby na określenie rodzaju i liczby systemów teleinformatycznych wchodzących w skład infrastruktury krytycznej).

Dowód akta kontroli str.: 78 – 80

W trakcie kontroli NIK, Dyrektor RCB przedstawił propozycję tematów prac Zespołu zadaniowego do spraw bezpieczeństwa cyberprzestrzeni Rzeczypospolitej Polskiej. Wśród zaproponowanej problematyki zawarto dokonanie przeglądu kryteriów pozwalających wyodrębnić obiekty, instalacje, urządzenia i usługi wchodzące w skład systemów infrastruktury krytycznej pod kątem ich wpływu na zapewnienie bezpieczeństwa cyberprzestrzeni.

Dowód akta kontroli tom II str.: 4

Zgodnie z art. 6 ust. 5 ustawy o zarządzaniu kryzysowemu, właściciele oraz posiadacze samoistni i zależni obiektów, instalacji lub urządzeń infrastruktury krytycznej[22] mają obowiązek ich ochrony, w szczególności przez przygotowanie i wdrażanie planów ochrony infrastruktury krytycznej. Przedmiotowe plany powinny zawierać m.in.: informacje na temat danego obiektu infrastruktury krytycznej, charakterystykę zagrożeń oraz zasadnicze warianty działania w sytuacji wystąpienia kryzysów[23].

Ustalono, iż w RCB nie opracowano narzędzi służących wspomaganiu kompletności i merytorycznej poprawności planów ochrony obiektów IK. Dyrektor RCB wyjaśnił, *(...) że na taką decyzję wpłynęły wątpliwości co do możliwości stworzenia takich narzędzi, biorąc pod uwagę przewidywaną dużą rozciągłość zawartości planów OIK zarówno w kwestii ich układu, jak i zakresu wykorzystania przez operatorów istniejących planów, procedur itp. Doświadczenia z oceny dotychczasowych planów OIK potwierdziły słuszność podjętej decyzji. Praktyką natomiast jest weryfikacja zawartości merytorycznej planów przez dwie osoby i w razie jakichkolwiek wątpliwości konsultacje z komórkami organizacyjnymi RCB np. zespołem informatyki i łączności"(...).*

Dowód akta kontroli: tom II str.: 17

Dyrektor RCB wyjaśnił również, że ocena kompletności i merytorycznej poprawności planów ochrony obiektów infrastruktury krytycznej w zakresie zabezpieczeń systemów teleinformatycznych jest dokonywana w oparciu o:

- przepisy rozporządzenia Rady Ministrów w sprawie planów ochrony infrastruktury krytycznej;
- dobre praktyki i rekomendacje dotyczące ochrony teleinformatycznej infrastruktury krytycznej zawarte w załączniku nr 2 do NPOIK;
- przygotowane przez RCB opracowanie pt. *Wskazówki do opracowania planów ochrony infrastruktury krytycznej*, w którym zawarto ramowe rekomendacje dotyczące zakresu tematycznego oraz trybu tworzenia planów ochrony infrastruktury krytycznej.

Dowód akta kontroli str.: 141 – 148, 263-266, 268-280

Ustalono, iż wg stanu na dzień 21 października 2014 r. Dyrektor RCB nie zatwierdził ani jednego planu ochrony infrastruktury krytycznej.

Dowód akta kontroli tom II str.: 8-9

---

[22] Zwani dalej operatorami infrastruktury krytycznej.

[23] Struktura planów oraz zasady tworzenia i uzgadniania ich treści zostały określone w rozporządzeniu Rady Ministrów z dnia 30 kwietnia 2010 r. w sprawie planów ochrony infrastruktury krytycznej (Dz. U. Nr 83, poz. 542 ze zm.).

Kontrola wykazała, że RCB monitorowało proces tworzenia planów ochrony infrastruktury krytycznej, pozyskując cyklicznie od operatorów infrastruktury krytycznej informacje na temat stopnia zaawansowania prac nad ww. dokumentami[24].

Dowód akta kontroli str.: 27, 141 – 142, 265,267, tom II str.: 8-9

***Zarządzenie nr 74 Prezesa Rady Ministrów.***

Na podstawie art. 7 ust. 4 ustawy o zarządzaniu kryzysowym, w dniu 12 października 2011 r., Prezes Rady Ministrów w zarządzeniu nr 74 określił wykaz przedsięwzięć i procedur systemu zarzadzania kryzysowego z uwzględnieniem zobowiązań wynikających z członkostwa w Organizacji Traktatu Północnoatlantyckiego oraz organy odpowiedzialne za ich uruchomienie.

Dowód: akta kontroli str.: 284

Kontrola wykazała, że Dyrektor RCB zrealizował obowiązek wynikający z § 6 ust. 2 ww. zarządzenia, tj. dokonał przeglądu wykazu przedsięwzięć i procedur systemu zarzadzania kryzysowego. W wyniku przeprowadzonego przeglądu opracowano projekt nowelizacji zarządzenia nr 74 obejmujący następujące zagadnienia związane z ochroną cyberprzestrzeni RP:

1. W załączniku nr 2 – Środki reagowania kryzysowego:

– doprecyzowano i wskazano wykonawców środków wynikających z NCRS[25] w obszarze ochrony infrastruktury krytycznej, zgodnie z ustawowymi zakresami ich kompetencji;

– rozszerzono załącznik o dodatkowy obszar zgłoszony przez ABW: *Systemy teleinformatyczne*, obejmujący zadania zapewnienia bezpieczeństwa systemów teleinformatycznych administracji państwowej.

2. W załączniku nr 5 – Stopnie alarmowe i stopnie alarmowe CRP określono cztery stopnie alarmowe CRP, wprowadzane w razie zagrożenia o charakterze terrorystycznym lub sabotażowym na systemy teleinformatyczne organów administracji publicznej lub systemy teleinformatyczne wchodzące w skład infrastruktury krytycznej oraz określono zadania do wykonania w ramach każdego z czterech ww. stopni alarmowych CRP.

Dowód: akta kontroli str.: 30-32

W dniu 19 września 2013 r. Dyrektor RCB przekazał do uzgodnień międzyresortowych projekt aktualizacji zarządzania nr 74 Prezesa Rady Ministrów wraz z 7 załącznikami, w tym projekt załącznika *stopnie alarmowe i stopnie alarmowe CRP*. W ramach uzgodnień resorty zgłosiły szereg uwag do ww. zarządzenia (ABW, MSW, MON i MAiC). Ze względu na dużą ilość uwag, Dyrektor RCB podjął decyzję, że w ramach obecnej aktualizacji do dalszego procedowania przekazany zostanie tylko załącznik nr 7, tj. *Procedura obiegu informacji na potrzeby zarządzania kryzysowego*. Pismo ze stosowną informacją zostało przesłane do resortów dnia 2 grudnia 2013 r.

Ustalono również, że w dniu 26 maja 2014 r. Dyrektor Rządowego Centrum Bezpieczeństwa przedstawił w trakcie odprawy Ministrowi Spraw Wewnętrznych projekt zarządzenia Prezesa Rady Ministrów zmieniającego *zarządzenie nr 74*

---

[24] Wg stanu na dzień 21 października 2014 r. zaawansowanie ww. prac przedstawia się następująco: 60 operatorów zakończyło prace związane z opracowaniem POIK, w 13 przypadkach prace nadal trwają. Aktualnie są realizowane procedury uzgodnienia 53 planów ze służbami i urzędami.

[25] NATO Crisis Response System -System Reagowania Kryzysowego NATO.

*Prezesa Rady Ministrów z dnia 12 października 2011 r.*, w tym m.in. projekt załącznika - *Stopnie alarmowe i stopnie alarmowe CRP* oraz – *Procedura obiegu informacji na potrzeby zarządzania kryzysowego.* Omówiono główne postanowienia przygotowanego dokumentu, po czym zdecydowano, że wymaga on dalszych prac analitycznych.

Dowód: akta kontroli str.: 170-207, 265

Kontrola wykazała, iż projekt zarządzenia zmieniającego zarządzenie nr 74 Prezesa Rady Ministrów z dnia 12 października 2011 r. w części zawierającej uzgodniony do tej pory projekt treści załącznika – *Procedura obiegu informacji na potrzeby zarządzania kryzysowego* - został przekazany[26] do ministrów i wojewodów, w celu ostatecznego uzgodnienia. W zakresie aktualizacji załącznika - *Stopnie alarmowe i stopnie alarmowe CRP* Dyrektor RCB wyjaśnił, iż *(...) przyjęcie przez Radę Ministrów zaktualizowanego KPZK stworzy ramy merytoryczne do doprecyzowania zapisu przedmiotowego załącznika do zarządzenia nr 74 Prezesa Rady Ministrów. Zgodnie z obowiązującym cyklem planowania przyjęcie KPZK powinno nastąpić w 2015 roku, po czym zostaną formalnie zakończone prace nad zmianą powyższego zarządzenia(...).*

Dowód: akta kontroli tom II str.: 28

Ustalone nieprawidłowości

W działalności kontrolowanej jednostki w przedstawionym wyżej zakresie nie stwierdzono nieprawidłowości

Uwagi dotyczące badanej działalności

NIK zwraca uwagę na fakt, iż pomimo, że systemy teleinformatyczne stanowią zasadniczą i integralną część infrastruktury krytycznej państwa, nie była podejmowana współpraca mająca na celu zapewnienie porównywalności i komplementarności wyników szacowania ryzyka prowadzonych przez RCB i MAiC odnośnie zagrożeń występujących w cyberprzestrzeni. Nie podejmowano również współpracy w celu modyfikacji kryteriów identyfikacji infrastruktury krytycznej, tak aby możliwe było precyzyjne określenie systemów teleinformatycznych, które wchodzą w skład wykazu infrastruktury krytycznej, w związku z czym w MAiC prowadzona jest obecnie równoległa, niezależna od prowadzonego przez RCB wykazu – kwerenda krytycznych systemów teleinformatycznych administracji rządowej. Kontrola wykazała także, że obowiązujące obecnie procedury systemu zarządzania kryzysowego w niewystarczającym stopniu uwzględniają zagrożenia dla systemów teleinformatycznych. W szczególności, wg stanu na 14 listopada 2014 r., w KPZK w ogóle nie określono zadań, podmiotów odpowiedzialnych oraz procedur reagowania na zagrożenia występujące w cyberprzestrzeni. Zdaniem NIK, brak spójności działań prowadzonych przez RCB i MAiC w zakresie ochrony krajowej teleinformatycznej infrastruktury krytycznej wynikał w szczególności z faktu, że wdrażanie systemu zarządzania kryzysowego zostało rozpoczęte znacznie wcześniej, niż działania systemowe mające na celu ochronę cyberprzestrzeni, co powoduje, że oba te procesy znajdują się w różnych stadiach zawansowania. Należy również podkreślić, że RCB nie otrzymywało żadnych wniosków, wskazówek, wytycznych, itp. ze strony Ministra Administracji i Cyfryzacji[27], który odpowiada za koordynację zadań związanych z ochroną cyberprzestrzeni RP i powinien inicjować działania mające na celu zapewnienie spójności i komplementarności wszystkich procesów związanych z ochroną teleinformatycznej infrastruktury krytycznej.

---

[26] Pismo nr WP.4163.1.1.2014.MS z dnia 15 października 2014 roku

[27] Wcześniej – Ministra Spraw Wewnętrznych i Administracji.

Ocena cząstkowa

NIK ocenia pozytywnie fakt, iż w ramach realizacji zadań wynikających z ustawy o zarządzaniu kryzysowym, RCB podejmowało działania związane z ochroną cyberprzestrzeni RP. Pozytywna ocena dotyczy w szczególności zamieszczenia w Załączniku nr 2 do NPOIK wskazówek dotyczących ochrony teleinformatycznej obiektów infrastruktury technicznej oraz opracowania projektu nowelizacji zarządzenia nr 74 Prezesa Rady Ministrów, w którym zaproponowano wprowadzenie stopni alarmowych związanych ze zdarzeniami występującymi w cyberprzestrzeni.

Ustalenia kontroli wykazały natomiast, że koordynowany przez RCB system zarządzania kryzysowego i ochrony infrastruktury krytycznej oraz budowany przez MAiC system ochrony cyberprzestrzeni RP są w praktyce rozłączne i nie uzupełniają się wzajemnie.

Uzgodnienia dotyczące określenia możliwych ram współpracy miedzy RCB a MAiC zostały rozpoczęte dopiero w trakcie niniejszej kontroli NIK. W trakcie kontroli, Dyrektor RCB podjął również działania zmierzające w kierunku zapewnienia spójności i komplementarności działań wynikających z zarządzania kryzysowego oraz ochrony cyberprzestrzeni RP, poprzez zgłoszenie propozycji do *prac Zespołu zadaniowego do spraw bezpieczeństwa cyberprzestrzeni Rzeczypospolitej Polskiej*, dotyczących: identyfikacji systemów infrastruktury krytycznej związanych z zachowaniem bezpieczeństwa w cyberprzestrzeni oraz ujednolicenia metodyk szacowania ryzyka.

# IV. Uwagi i wnioski

W opinii NIK, uzależnienie krytycznej infrastruktury państwa od systemów teleinformatycznych powoduje potrzebę bieżącego aktualizowania dokumentów i procedur zarządzania kryzysowego pod kątem nowych i dynamicznie wzrastających zagrożeń związanych ze zdarzeniami występującymi w cyberprzestrzeni. W związku z powyższym zasadne jest zapewnienie spójności i komplementarności działań prowadzonych przez RCB w ramach zarzadzania kryzysowego z działaniami MAiC oraz zdefiniowanie roli RCB w ramach systemu ochrony cyberprzestrzeni RP budowanego przez Ministra Administracji i Cyfryzacji.

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[28], wnosi o:

1) podjęcie, w uzgodnieniu z Ministrem Administracji i Cyfryzacji, działań mających na celu zdefiniowanie roli i zadań Dyrektora Rządowego Centrum Bezpieczeństwa w ramach budowanego systemu ochrony cyberprzestrzeni RP.

# V. Pozostałe informacje i pouczenia

Prawo zgłoszenia zastrzeżeń

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

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

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

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 17.11.2014 r.

Najwyższa Izba Kontroli

Departament Porządku
i Bezpieczeństwa Wewnętrznego

Kontrolerzy

Mariusz Mijewski

Główny specjalista k.p.

1. ..... *Podpis*

Adam Zakrzewski

Główny specjalista k.p.

2. ..... *Podpis*

Mariusz Perzyna

Specjalista k.p.

3. ..... *Podpis*

Dyrektor

Marek Bieńkowski

DYREKTOR
Departament Porządku
i Bezpieczeństwa Wewnętrznego

..... Marek Bieńkowski .....

*podpis*