KPB-4101-002-00/2014
Nr ewid. 42/2015/P/14/043/KPB

Informacja o wynikach kontroli

REALIZACJA PRZEZ PODMIOTY PAŃSTWOWE ZADAŃ W ZAKRESIE OCHRONY CYBERPRZESTRZENI RP

DEPARTAMENT PORZĄDKU
I BEZPIECZEŃSTWA WEWNĘTRZNEGO

MISJĄ

Najwyższej Izby Kontroli jest dbałość o gospodarność i skuteczność w służbie publicznej dla Rzeczypospolitej Polskiej

WIZJĄ

Najwyższej Izby Kontroli jest cieszący się powszechnym autorytetem najwyższy organ kontroli państwowej, którego raporty będą oczekiwanym i poszukiwanym źródłem informacji dla organów władzy i społeczeństwa

Dyrektor Departamentu Porządku
i Bezpieczeństwa Wewnętrznego
Marek Bieńkowski

Akceptuję:
Wojciech Kutyła

Wiceprezes Najwyższej Izby Kontroli

Zatwierdzam:
Krzysztof Kwiatkowski

Prezes Najwyższej Izby Kontroli
Warszawa, dnia 23.06.2015 r.

Najwyższa Izba Kontroli
ul. Filtrowa 57
02-056 Warszawa
T/F +48 22 444 50 00

www.nik.gov.pl

Spis treści

Okładka: Materiały NIK

Wykaz stosowanych skrótów i pojęć

ACTA	Międzynarodowe porozumienie dotyczące walki z naruszaniem własności intelektualnej.
Ataki ACTA	Ataki wymierzone w styczniu 2012 r. w najważniejsze strony internetowe administracji publicznej w ramach kampanii protestu społecznego związanej z pracami, mającymi na celu podpisanie przez Polskę porozumienia ACTA.
Atak DDoS	Atak na system komputerowy lub usługę sieciową w celu uniemożliwienia działania poprzez generowanie bardzo dużej ilości fałszywych połączeń, skutkujących przeciążaniem serwera, który np. obsługuje stronę internetową.
ARAKIS.GOV	System wczesnego ostrzegania przed zagrożeniami w sieci Internet.
Botnet	Sieć zainfekowanych komputerów sterowanych centralnie przez specjalne kontrolery, które są używane do różnego rodzaju wrogiej działalności, bez wiedzy ich właścicieli.
CERT	Zespół ekspertów do spraw bezpieczeństwa informatycznego, których głównym zadaniem jest reagowanie na incydenty z zakresu bezpieczeństwa komputerowego. Świadczy on usługi niezbędne do rozwiązania tego typu problemów oraz umożliwienia użytkownikom wznowienia normalnej działalności.
CERT.GOV.PL	Rządowy zespół reagowania na incydenty komputerowe, funkcjonujący w Agencji Bezpieczeństwa Wewnętrznego.
CERT Polska	Zespół reagowania na incydenty komputerowe funkcjonujący w ramach NASK pełniący, zgodnie z terminologią wykorzystywaną przez ENISA, rolę nieformalnego – „De facto" narodowego Zespołu CERT.
CRP	Cyberprzestrzeń Rzeczypospolitej Polskiej.
Cyberprzestrzeń	Przestrzeń przetwarzania i wymiany informacji tworzona przez systemy teleinformatyczne wraz z powiązaniami między nimi oraz relacjami z użytkownikami.
Ćwiczenia	Działania mające na celu praktyczną weryfikację, w warunkach zbliżonych do rzeczywistych, stosowania przyjętych i opanowanych procedur i metod postępowania w sytuacji zagrożenia lub wystąpienia incydentu bezpieczeństwa.
Dyrektywa NIS	Dyrektywa Parlamentu Europejskiego i Rady Unii Europejskiej w sprawie środków mających na celu zapewnienie wspólnego wysokiego poziomu bezpieczeństwa sieci i informacji w obrębie Unii Europejskiej.
ENISA	Europejska Agencja ds. Bezpieczeństwa Sieci i Informacji.
Incydent	Pojedyncze zdarzenie lub seria niepożądanych lub niespodziewanych zdarzeń związanych z bezpieczeństwem informacji, które stwarzają znaczne prawdopodobieństwo zakłócenia prowadzonych działań i zagrażają bezpieczeństwu informacji.

Infrastruktura Krytyczna	Systemy oraz wchodzące w ich skład powiązane ze sobą funkcjonalnie obiekty (w tym budowlane), urządzenia, instalacje, usługi kluczowe dla bezpieczeństwa państwa i jego obywateli oraz służące zapewnieniu sprawnego funkcjonowania organów administracji publicznej, a także instytucji i przedsiębiorców.
ISO	Międzynarodowa Organizacja Normalizacyjna.
KPZK	Krajowy Plan Zarządzania Kryzysowego.
Krytyczna Infrastruktura Teleinformatyczna	Systemy i sieci teleinformatyczne niezbędne dla prowadzenia podstawowych działań gospodarczych i funkcjonowania instytucji publicznych państwa.
MIL-CERT.PL	Wojskowy zespół reagowania na incydenty komputerowe, funkcjonujący w ramach resortu obrony narodowej.
NASK	Naukowa i Akademicka Sieć Komputerowa – instytut badawczy.
NPOIK	Narodowy Program Ochrony Infrastruktury Krytycznej.
Operator Infrastruktury Krytycznej	Podmiot będący właścicielem, posiadaczem samoistnym lub zależnym obiektów, instalacji, urządzeń i usług wchodzących w skład infrastruktury krytycznej.
Phishing	Tworzenie stron podszywających się pod banki, sklepy internetowe, itp., mające na celu wprowadzenie w błąd ich użytkownika.
Podatność	Słabość systemu informatycznego lub jego zabezpieczeń, która może być wykorzystana przez napastników.
Polityka	„Polityka Ochrony Cyberprzestrzeni RP" przyjęta przez Radę Ministrów w dniu 25 czerwca 2013 r.
Rozporządzenie w sprawie krajowych ram interoperacyjności	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.
SRnIK	System reagowania na incydenty komputerowe resortu obrony narodowej.
System Teleinformatyczny	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.
Testy	Czynności weryfikujące funkcjonalność i poziom zabezpieczeń, np. systemu teleinformatycznego.
Ustawa o informatyzacji	Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne.

WPROWADZENIE

Postępujący rozwój techniki i metod wymiany informacji, obok wielu niewątpliwych korzyści, wymusza zmianę sposobu rozumienia pojęcia bezpieczeństwa. **Dotychczasowe „fizyczne" zagrożenia towarzyszące ludziom od zamierzchłych czasów, postęp nauki i technologii uzupełnił o nowy ich rodzaj – zagrożenia teleinformatyczne. Gwałtowne i niespodziewane ich powstanie spowodowało zachwianie istniejącego modelu bezpieczeństwa państw, instytucji, przedsiębiorców oraz obywateli**. Model ten kształtowany i udoskonalany przez wieki obligował:

- państwa do tworzenia rozbudowanych struktur siłowych zdolnych do odparcia napaści zewnętrznej oraz utrzymania ładu i porządku wewnętrznego;
- instytucje i przedsiębiorców do wydzielania w swoich budżetach środków na ochronę fizyczną, systemy kamer i inne atrybuty bezpieczeństwa;
- zwykłych obywateli do ochrony i ubezpieczania swojego mienia oraz współfinansowania struktur siłowych państwa.

Cały ten wypracowany i doskonalony przez stulecia mechanizm bezpieczeństwa został stosunkowo niedawno postawiony w obliczu zupełnie nowego rodzaju zagrożeń. Zagrożeń tym bardziej niebezpiecznych, że oddziaływują one skrycie, są stosunkowo łatwe do wytworzenia, mogą pochodzić z wielu różnych źródeł, a ich natura ulega ciągłym zmianom.

Analizując polski system bezpieczeństwa łatwo można zidentyfikować: wielotysięczną armię posługującą się różnymi systemami uzbrojenia, Policję o strukturze obejmującej cały kraj, szereg innych służb i formacji, czy też liczną grupę najemnych pracowników firm ochroniarskich. Widoczne są również te wszystkie atrybuty bezpieczeństwa, z którymi obcujemy codziennie: płoty, bramy, kraty i zamki. Jednak próba wskazania struktur chroniących przed zagrożeniami związanymi z wykorzystywaniem cyberprzestrzeni napotyka na trudności. Z jednej strony przyzwyczailiśmy się już do rozpoczynania pracy poprzez podanie hasła do komputera – wpisujemy je też w wirtualnych sklepach, bankach, hotelach, czy kawiarenkach. Większość z nas obawia się wirusów komputerowych i słyszała kiedyś słowo „haker". Czy jednak mamy poczucie, że w przypadku realnej szkody spowodowanej przez tegoż hakera lub wirus, mamy gdzie się zwrócić o pomoc? Czy istnieje jakiś państwowy „komisariat", który przyjmie od nas zgłoszenie? Czy są gdzieś „wirtualni strażacy" gotowi nieść pomoc w przypadku informatycznej katastrofy? Czy jako państwo jesteśmy chronieni przed wywołanym z zewnątrz wirtualnym paraliżem, który spotkał już kiedyś jednego z naszych sąsiadów?

W ramach niniejszej kontroli, NIK podjęła zatem próbę szerszego spojrzenia na ten nowy aspekt bezpieczeństwa oraz oceny funkcjonujących w tym obszarze struktur państwowych. Przeprowadzona kontrola miała na celu zweryfikowanie istnienia systemu, za pomocą którego państwo jest gotowe ochraniać swoje kluczowe zasoby oraz swoich obywateli przed zagrożeniami występującymi w cyberprzestrzeni.

1 ZAŁOŻENIA KONTROLI

Kontrola planowa nr P/14/043 – „Realizacja przez podmioty państwowe zadań w zakresie ochrony cyberprzestrzeni Rzeczypospolitej Polskiej".

Cel główny kontroli

Głównym celem kontroli było sprawdzenie, w jaki sposób administracja państwowa zarządza ryzykiem związanym z zagrożeniami występującymi w cyberprzestrzeni RP.

Cele cząstkowe

Celami cząstkowymi kontroli było uzyskanie odpowiedzi na następujące pytania:

1. Czy został opracowany spójny system działań organów administracji państwowej, mający na celu monitorowanie zagrożeń występujących w cyberprzestrzeni RP, przeciwdziałanie im oraz minimalizowanie skutków incydentów? W szczególności: czy określono ramy prawne tego systemu, dokonano podziału kompetencji między jego uczestnikami, przydzielono im niezbędne zasoby, określono mechanizmy koordynacji i wymiany informacji oraz sformułowano krajowy zbiór dobrych praktyk?
2. Czy funkcjonujące w Polsce rozwiązania instytucjonalno-prawne zapewniają skuteczne szacowanie ryzyk związanych z zagrożeniami występującymi w cyberprzestrzeni?
3. Czy obowiązujące obecnie regulacje prawne oraz działania realizowane przez podmioty państwowe w zakresie bezpieczeństwa systemów teleinformatycznych są spójne, kompletne oraz odwołują się do uznanych międzynarodowych wzorów dobrych praktyk?

Podstawa prawna, kryteria

Kontrolę przeprowadzono na podstawie art. 2 ust. 1 ustawy o NIK[1], zgodnie z kryteriami określonymi w art. 5 ust. 1 ustawy, tj. legalności, gospodarności, celowości i rzetelności.

Zakres przedmiotowy kontroli

Kontrolą objęto realizację zadań podmiotów administracji państwowej w zakresie bezpieczeństwa teleinformatycznego, obejmujących w szczególności: szacowanie ryzyka dla zdarzeń występujących w cyberprzestrzeni, budowę krajowego systemu ochrony cyberprzestrzeni, reagowanie na incydenty komputerowe, mechanizmy współpracy z innymi (w tym komercyjnymi) użytkownikami i administratorami cyberprzestrzeni, działania szkoleniowe i edukacyjne. Zadania realizowane przez poszczególne podmioty zostały ocenione z zastosowaniem wyznaczników wynikających z przepisów prawa oraz wzorów dobrych praktyk wypracowanych między innymi przez wyspecjalizowane instytucje międzynarodowe oraz podmioty komercyjne wiodące w obszarze bezpieczeństwa teleinformatycznego[2].

Badania kontrolne nie dotyczyły bezpieczeństwa teleinformatycznego poszczególnych podmiotów, ani wykorzystywanych przez nie systemów informatycznych[3].

1 Ustawa z dnia 23 grudnia 1994 r. o Najwyższej Izbie Kontroli (Dz. U. z 2012 r., poz. 82 ze zm.), zwana dalej „ustawą o NIK".

2 Zbiór dobrych praktyk zdefiniowanych w obszarze ochrony cyberprzestrzeni został określony w Załączniku nr 1 do informacji.

3 Bezpieczeństwo danych, przetwarzanych w wybranych systemach teleinformatycznych wykorzystywanych do realizacji istotnych zadań publicznych, będzie przedmiotem kontroli przewidzianej w Planie Pracy NIK na 2015 r.

Zakres podmiotowy kontroli

Kontrolą objęto 8 podmiotów państwowych, którym przypisano kluczowe zadania związane z bezpieczeństwem teleinformatycznym państwa, tj.: Ministerstwo Administracji i Cyfryzacji, Agencję Bezpieczeństwa Wewnętrznego, Ministerstwo Obrony Narodowej, Ministerstwo Spraw Wewnętrznych, Naukową i Akademicką Sieć Komputerową, Urząd Komunikacji Elektronicznej, Rządowe Centrum Bezpieczeństwa oraz Komendę Główną Policji. W informacji uwzględniono również wyniki analizy dokumentacji i wyjaśnień uzyskanych na etapie analizy przedkontrolnej oraz w trakcie kontroli, od podmiotów niekontrolowanych, w trybie art. 29 ust. 1 pkt 2 lit. f ustawy o NIK[4].

Okres objęty kontrolą

Kontrolę przeprowadzono od 2 czerwca 2014 r. do 5 grudnia 2014 r. Badaniem objęto okres od początku 2008 r. do dnia zakończenia czynności kontrolnych.

[4] Informacje w ww. trybie uzyskano z: Kancelarii Prezesa Rady Ministrów, Ministerstwa Finansów, Ministerstwa Infrastruktury i Rozwoju, Ministerstwa Nauki i Szkolnictwa Wyższego, Narodowego Centrum Badań i Rozwoju, Rządowego Centrum Legislacji oraz od podmiotów będących beneficjentami projektów naukowo-badawczych dotyczących bezpieczeństwa teleinformatycznego, tj. Akademii Górniczo-Hutniczej, Wojskowego Instytutu Łączności oraz Instytutu Łączności.

2 PODSUMOWANIE WYNIKÓW KONTROLI

2.1 Ogólna ocena kontrolowanej działalności

Najwyższa Izba Kontroli ocenia negatywnie realizację zadań podmiotów państwowych w zakresie ochrony cyberprzestrzeni RP.

Administracja państwowa nie podjęła dotychczas niezbędnych działań, mających na celu zapewnienie bezpieczeństwa teleinformatycznego Polski. Pomimo tego, że coraz większa część usług publicznych oraz istotnych aspektów życia społecznego i gospodarczego realizowanych jest obecnie w sieci Internet lub z wykorzystaniem systemów teleinformatycznych, bezpieczeństwo Polski w dalszym ciągu jest postrzegane jedynie w sposób konwencjonalny[5]. Nie dostrzeżono, że powstała nowa kategoria zagrożeń, wymagająca pilnej reakcji państwa. Kierownictwo najważniejszych instytucji publicznych nie było świadome niebezpieczeństw związanych z funkcjonowaniem cyberprzestrzeni oraz wynikających z tego faktu nowych zadań administracji państwowej. W rezultacie:

- **nie podjęto dotychczas spójnych i systemowych działań, mających na celu monitorowanie i przeciwdziałanie zagrożeniom występującym w cyberprzestrzeni oraz minimalizowanie skutków incydentów;**
- **nie oszacowano ryzyk dla krajowej infrastruktury teleinformatycznej oraz nie wypracowano narodowej strategii ochrony cyberprzestrzeni, stanowiącej podstawę dla działań podnoszących bezpieczeństwo teleinformatyczne;**
- **nie określono struktury i ram prawnych krajowego systemu ochrony cyberprzestrzeni, nie zdefiniowano obowiązków i uprawnień jego uczestników oraz nie przydzielono zasobów niezbędnych do skutecznej realizacji zadań;**
- **nie przygotowano procedur reagowania w sytuacjach kryzysowych związanych z cyberprzestrzenią.**

Działania podmiotów państwowych związane z ochroną cyberprzestrzeni były prowadzone w sposób rozproszony i bez spójnej wizji systemowej. Sprowadzały się one do doraźnego, ograniczonego reagowania na bieżące wydarzenia oraz biernego oczekiwania na rozwiązania, które w tym obszarze zaproponuje Unia Europejska. Kluczowym czynnikiem paraliżującym aktywność państwa w tym zakresie był brak jednego ośrodka decyzyjnego, koordynującego działania innych instytucji publicznych.

Przedstawiona ocena dotyczy braku systemowych działań w zakresie ochrony cyberprzestrzeni RP, natomiast nie odnosi się ona do stanu bezpieczeństwa teleinformatycznego poszczególnych podmiotów, ani wykorzystywanych przez nie systemów, które to zagadnienia nie były przedmiotem niniejszej kontroli.

Odpowiedzialność za ustalony w toku kontroli brak, w latach 2008–2014, systemowych działań w zakresie ochrony cyberprzestrzeni RP ponoszą osoby kierujące w tym okresie podmiotami realizującymi zadania związane z bezpieczeństwem teleinformatycznym państwa. W ocenie NIK, istotnym czynnikiem wpływającym negatywnie na realizację zadań w tym obszarze, było także niewystarczające zaangażowanie najwyższego kierownictwa administracji rządowej, w tym w szczególności Prezesa Rady Ministrów. Było ono szczególnie potrzebne do rozstrzygania kwestii spornych między poszczególnymi urzędami, ujawnionych

[5] Tj. jako działania z zakresu zapobiegania i reagowania na tradycyjne zagrożenia, takie np. jak: powodzie, pożary, akty terroru z wykorzystaniem przemocy fizycznej, tradycyjne konflikty zbrojne, itd.

w trakcie konsultacji międzyresortowych kolejnych[6], rządowych projektów narodowej strategii ochrony cyberprzestrzeni oraz zapewnienia współdziałania organów i instytucji związanych z bezpieczeństwem teleinformatycznym państwa.

Jako działania pozytywne w obszarze ochrony cyberprzestrzeni można wskazać jedynie fragmentaryczne inicjatywy poszczególnych instytucji objętych kontrolą, w tym w szczególności:

- powołanie i utrzymywanie na wysokim poziomie zespołów CERT przez takie instytucje jak NASK, ABW oraz MON;
- utworzenie przez Ministra Obrony Narodowej systemu reagowania na incydenty komputerowe w resorcie obrony narodowej oraz wyspecjalizowanej jednostki – Narodowego Centrum Kryptologii;
- upowszechnianie przez RCB wytycznych i dobrych praktyk z zakresu ochrony teleinformatycznej infrastruktury krytycznej;
- prowadzenie przez NASK i Policję aktywnych działań edukacyjnych dotyczących m.in. przestępczości komputerowej i bezpieczeństwa w cyberprzestrzeni.

Oceny poszczególnych podmiotów objętych kontrolą

Kontrola wykazała, że Minister Administracji i Cyfryzacji, będący w chwili obecnej jedynym organem administracji publicznej, któremu bezpośrednio przypisano obowiązki związane z ochroną cyberprzestrzeni, nie realizował należących do niego zadań w zakresie inicjowania i koordynowania działań innych podmiotów w obszarze bezpieczeństwa teleinformatycznego państwa. W związku z powyższym, NIK negatywnie oceniła[7] dotychczasową realizację zadań Ministra Administracji i Cyfryzacji we wszystkich trzech obszarach objętych kontrolą, tj. w zakresie:

- budowy systemu ochrony cyberprzestrzeni RP;
- szacowania ryzyk związanych ze zdarzeniami występującymi w cyberprzestrzeni;
- realizacji zadań związanych z ochroną cyberprzestrzeni.

Dokonując oceny pozostałych 7 jednostek objętych kontrolą[8], NIK uwzględniła fakt, iż nie zostały dotychczas precyzyjnie przypisane i zdefiniowane zadania poszczególnych instytucji publicznych dotyczące bezpieczeństwa teleinformatycznego państwa. Ponadto w działalności niektórych podmiotów (np. UKE) stwierdzono problemy systemowe, występujące niezależne od działań Kierownictwa tych jednostek. W związku z powyższym odstąpiono od sformułowania ocen wg tradycyjnej trójstopniowej skali i zastosowano tzw. oceny opisowe. W przypadku poszczególnych skontrolowanych podmiotów NIK oceniła, w szczególności, iż:

---

6 W latach 2008–2011 opracowano siedem kolejnych, niezatwierdzonych projektów narodowej strategii bezpieczeństwa cyberprzestrzeni.

7 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.

8 MSW, UKE, RCB, KGP, MON, ABW, NASK.

1. **Minister Spraw Wewnętrznych nie realizował żadnych zadań związanych z budową krajowego systemu ochrony cyberprzestrzeni**. Działania Ministra w obszarze bezpieczeństwa IT ograniczały się do własnych sieci oraz systemów resortowych i były prowadzone w sposób nierzetelny. Minister nie wykonywał również swoich obowiązków, wynikających z ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne, dotyczących kontroli systemów teleinformatycznych oraz z „Polityki Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej" (zwanej dalej „Polityką").
2. Obowiązujące obecnie **przepisy Prawa telekomunikacyjnego są wadliwie sformułowane i nie mogą być w praktyce wykorzystywane w ramach realizacji zadań związanych z bezpieczeństwem IT**, co było przyczyną **braku wykonywania obowiązków Prezesa Urzędu Komunikacji Elektronicznej**, dotyczących w szczególności pozyskiwania informacji o incydentach występujących w cyberprzestrzeni oraz informowania obywateli o zagrożeniach związanych z korzystaniem z Internetu.
3. **Koordynowany przez Rządowe Centrum Bezpieczeństwa system zarządzania kryzysowego nie jest komplementarny i spójny z działaniami w zakresie bezpieczeństwa teleinformatycznego oraz w niewystarczającym stopniu uwzględnia nowe zagrożenia dla infrastruktury krytycznej państwa, jakimi są zagrożenia występujące w cyberprzestrzeni**.
4. **Jednostki organizacyjne Policji podejmowały działania związane ze zwalczaniem przestępczości komputerowej oraz aktywnie uczestniczyły w kampaniach edukacyjno-informacyjnych** dotyczących bezpiecznego korzystania z Internetu. **Komendant Główny Policji nie podjął natomiast rzetelnych działań w celu wdrożenia w Policji realnego i kompleksowego systemu reagowania na zagrożenia i incydenty w cyberprzestrzeni.** Stwierdzono także opóźnienia oraz brak realizacji części zadań wynikających z „Polityki".
5. **Minister Obrony Narodowej aktywnie realizował zadania w zakresie budowy resortowego systemu reagowania na incydenty komputerowe** oraz uczestniczył w budowie krajowego systemu ochrony cyberprzestrzeni. **W działalności MON zidentyfikowano jednak liczne problemy i ryzyka o charakterze systemowym, wskazujące na brak rzetelnego przygotowania działań Ministra oraz stwarzające zagrożenie dla ich skutecznej realizacji.**
6. **Kierownictwo Agencji Bezpieczeństwa Wewnętrznego** realizowało zadania związane z zapobieganiem i reagowaniem na incydenty komputerowe w systemach podmiotów administracji państwowej, polegające m.in. na **stworzeniu i utrzymywaniu systemu wczesnego ostrzegania ARAKIS.GOV oraz Zespołu CERT.GOV.PL. Aktywność ABW podlegała istotnym ograniczeniom wynikającym w szczególności z niewystarczających zasobów i braku formalnego umocowania Zespołu CERT.GOV.PL.**
7. **Kierownictwo Naukowej i Akademickiej Sieci Komputerowej** podejmowało liczne działania, które NIK oceniła jako **dobre praktyki** w zakresie ochrony cyberprzestrzeni. Dotyczyły one w szczególności powołania i utrzymywania zespołu **CERT Polska. Działania NASK miały jednak charakter tymczasowy i nieformalny oraz były ściśle związane z realizowanymi przez ten podmiot procesami biznesowymi i podlegały wynikającym z tego faktu ograniczeniom, w tym finansowym.**

2.2 Synteza wyników kontroli

1. **Rada Ministrów i kierownictwo podmiotów administracji państwowej nie opracowały narodowej strategii ochrony cyberprzestrzeni Polski, która mogłaby być podstawą konkretnych, systemowych działań podnoszących poziom bezpieczeństwa teleinformatycznego państwa.** Prace nad strategią były prowadzone od 2008 r., natomiast ze względu na ich nierzetelne przygotowanie i sprzeczne interesy różnych instytucji biorących w nich udział, kolejne wersje tego dokumentu nie były zatwierdzone. **Dopiero w czerwcu 2013 r. Rada Ministrów przyjęła „Politykę Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej" – dokument będący wynikiem braku porozumienia i źle rozumianego kompromisu, o niskiej jakości, nieprecyzyjny i obarczony wieloma błędami merytorycznymi. Nieliczne zadania wynikające bezpośrednio z „Polityki" nie były realizowane przez większość skontrolowanych przez NIK podmiotów, co pozwala stwierdzić, że jej praktyczne zastosowanie w celu poprawy bezpieczeństwa teleinformatycznego państwa było jedynie symboliczne.**

(szerzej str. 34–39)

2. **Kierownictwo większości objętych kontrolą podmiotów państwowych, w tym w szczególności Minister Administracji i Cyfryzacji odpowiadający za koordynację działań w obszarze bezpieczeństwa teleinformatycznego, nie miało świadomości należących do nich zadań związanych z ochroną cyberprzestrzeni RP, wynikających m.in. z kierowania sprawami zarządzania kryzysowego, informatyzacji, czy łączności.** Zapewnienie bezpieczeństwa państwa w dalszym ciągu postrzegane było przez nich w sposób konwencjonalny, głównie poprzez wdrożenie środków ochrony fizycznej, bez uwzględnienia postępujących zmian technologicznych i wzrostu zagrożeń w cyberprzestrzeni. **W rezultacie kontrolowane jednostki nie realizowały żadnych zadań w celu poprawy bezpieczeństwa teleinformatycznego państwa lub działały fragmentarycznie i z dużym opóźnieniem, ograniczając się jedynie do zabezpieczania własnych witryn internetowych, sieci i systemów teleinformatycznych.**

(szerzej str. 39–40, 62–63, 65)

3. **Do końca okresu objętego kontrolą nie opracowano założeń systemu finansowania działań związanych z ochroną cyberprzestrzeni RP.** Zgodnie ze stanowiskiem Ministra Finansów wskazującym na konieczność „bezkosztowego" wykonywania tych zadań, **nie zostały również przydzielone żadne dodatkowe środki finansowe na ich realizację, co w ocenie NIK, praktycznie sparaliżowało działania podmiotów państwowych w zakresie bezpieczeństwa teleinformatycznego. Zasoby poszczególnych jednostek objętych kontrolą były nieadekwatne do przypisanych im obowiązków. Należy przy tym jednak zauważyć, że żaden z tych podmiotów nie przeprowadził rzetelnego oszacowania środków (ludzkich, rzeczowych i finansowych) niezbędnych do efektywnej realizacji działań w zakresie ochrony cyberprzestrzeni.**

(szerzej str. 40–44)

4. **Nie były dotychczas prowadzone żadne prace legislacyjne mające na celu unormowanie zagadnień związanych z bezpieczeństwem teleinformatycznym państwa.** Nie przeprowadzono inwentaryzacji rozproszonych w różnych aktach prawnych przepisów związanych z cyberbezpieczeństwem oraz nie zdefiniowano pożądanych kierunków zmian legislacyjnych. Nie przygotowano nawet założeń aktu normatywnego określającego strukturę krajowego systemu ochrony cyberprzestrzeni i jego uczestników. **Zadania podmiotów**

państwowych związane z bezpieczeństwem teleinformatycznym były rozproszone, a obowiązujące w tym zakresie przepisy nieprecyzyjne, nieadekwatne lub też w ogóle nie stosowane w praktyce. Brak działań administracji państwowej w tym obszarze wynikał m.in. z biernego oczekiwania na propozycje legislacyjne Unii Europejskiej.

(szerzej str. 44–46)

5. **Działania podmiotów państwowych w zakresie ochrony cyberprzestrzeni były prowadzone w sposób niespójny, bez rzetelnego planowania, przygotowania i jednolitej wizji systemowej.** W całym okresie objętym kontrolą, zarówno na szczeblu ogólnokrajowym, jak i w przypadku poszczególnych jednostek objętych badaniem, **nie zostały określone cele, produkty, mierniki i terminy realizacji zadań związanych z ochroną cyberprzestrzeni RP. Nie opracowano również projektów szczegółowych**, które zgodnie z zapisami „Polityki", miały służyć wdrażaniu tego dokumentu w poszczególnych obszarach związanych z poprawą bezpieczeństwa teleinformatycznego.

(szerzej str. 46–47)

6. **Podmioty administracji państwowej nie prowadziły rzetelnej i efektywnej współpracy w zakresie ochrony cyberprzestrzeni RP oraz nie wdrożono skutecznych mechanizmów koordynacji działań w tym obszarze.** Kierownictwo kontrolowanych podmiotów nie prowadziło aktywnej współpracy z innymi instytucjami, którym przypisano obowiązki związane z bezpieczeństwem teleinformatycznym oraz w ograniczonym zakresie współpracowało z Ministrem Administracji i Cyfryzacji, odpowiadającym za koordynację tych działań. **Minister Administracji i Cyfryzacji nie dysponował zasobami pozwalającymi na realną realizację zadań dotyczących zarządzania krajowym systemem ochrony cyberprzestrzeni oraz nie miał uprawnień w zakresie oddziaływania na inne instytucje, które odmawiały współpracy lub nierzetelnie i nieterminowo wywiązywały się z przypisanych im obowiązków. Istotnym czynnikiem ograniczającym efektywność współpracy było również niepowołanie przez Prezesa Rady Ministrów, ustanowionego w „Polityce", międzyresortowego zespołu mającego wspierać Ministra Administracji i Cyfryzacji w koordynacji działań związanych z podnoszeniem bezpieczeństwa teleinformatycznego.**

(szerzej str. 48–49)

7. **W całym okresie objętym kontrolą, pomimo podjęcia licznych działań i zaangażowania dużych zasobów, nie zostało przeprowadzone rzetelne i kompleksowe oszacowanie ryzyk związanych ze zdarzeniami występującymi w cyberprzestrzeni.** Wyniki analiz ryzyka prowadzonych w oparciu o przepisy dotyczące zarządzania kryzysowego oraz Prawa telekomunikacyjnego **wykazały, że w dalszym ciągu zagrożenia związane z bezpieczeństwem teleinformatycznym nie są postrzegane, jako istotne i mające bezpośredni wpływ na infrastrukturę państwa. W przypadku procesów szacowania ryzyka koordynowanych przez Ministra Administracji i Cyfryzacji, ze względu na ich nierzetelne przygotowanie i przeprowadzenie oraz zawężony zakres podmiotowy, uzyskane wyniki były niekompletne i w znacznym stopniu nieużyteczne.** Nie zapewniły one realnej wiedzy na temat kluczowej infrastruktury teleinformatycznej państwa, prawdopodobieństwa wystąpienia zagrożeń oraz pożądanych metod zarządzania ryzykiem. **Brak kompleksowej i rzetelnej analizy ryzyka, uniemożliwił planowanie oraz realizację dalszych działań mających na celu ochronę cyberprzestrzeni.**

(szerzej str. 50–52, 65)

8. **W Polsce nie funkcjonuje krajowy system reagowania na incydenty komputerowe.** Czynności z zakresu reagowania na incydenty są realizowane przez funkcjonujące niezależnie od siebie państwowe i prywatne zespoły CERT, zajmujące się swoimi własnymi obszarami oddziaływania. **Kierownictwo administracji państwowej nie podejmowało natomiast działań w celu wypracowania założeń pożądanej struktury zespołów reagowania, ustanowienia kanałów wymiany informacji oraz powołania CERTu narodowego**, koordynującego działania tych podmiotów i odpowiadającego za współpracę międzynarodową. **Minister Administracji i Cyfryzacji, który zgodnie z zapisami Polityki odpowiada za koordynację krajowego systemu reagowania na incydenty komputerowe, nie realizował żadnych zadań w tym zakresie. Administracja państwowa nie dysponuje również wiedzą na temat skali i rodzaju incydentów występujących w cyberprzestrzeni, a ustanowiony w Prawie telekomunikacyjnym system zbierania i rejestrowania takich informacji okazał się być całkowicie nieskuteczny.**

(szerzej str. 53–59)

9. **Podmioty administracji państwowej nie podejmowały rzetelnych i adekwatnych działań w celu ustanowienia wymogów w zakresie bezpieczeństwa cyberprzestrzeni.** Zdefiniowane w toku kontroli wytyczne i wzory dobrych praktyk dotyczące bezpieczeństwa teleinformatycznego nie miały spójnego, systemowego charakteru i stanowiły reakcje ad hoc (np. na konkretne wydarzenia społeczne) lub były ograniczone do własnych witryn internetowych, systemów i sieci resortowych. **Nie podejmowano również wymaganych przepisami prawa działań dotyczących kontroli przestrzegania ustanowionych wymogów z zakresu bezpieczeństwa teleinformatycznego. Podmioty państwowe w ogóle nie wykonywały w tym zakresie obowiązków wynikających z ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne.**

(szerzej str. 59–62)

10. **Nie zostały dotychczas opracowane plany reagowania kryzysowego i utrzymania ciągłości działania podstawowych procesów ekonomicznych oraz funkcji państwa, w sytuacjach zagrożeń związanych z cyberprzestrzenią. Tworzone w Polsce plany kryzysowe, w tym w szczególności Krajowy Plan Zarządzania Kryzysowego, odnosiły się wyłącznie do konwencjonalnych zdarzeń, takich jak np. katastrofy naturalne i nie uwzględniały zmiany charakteru zagrożeń wynikającej m.in. z postępu technologicznego.** Obowiązujące przepisy dotyczące zarządzania kryzysowego oraz Prawa telekomunikacyjnego nie były wykorzystywane w celu opracowania schematów działania w sytuacjach kryzysowych związanych z cyberprzestrzenią, a Kierownictwo odpowiedzialnych podmiotów państwowych nie dostrzegało potrzeby podjęcia działań w tym zakresie.

(szerzej str. 62-65)

11. **Objęte kontrolą podmioty, w tym w szczególności Minister Administracji i Cyfryzacji odpowiadający za koordynację działań w zakresie ochrony cyberprzestrzeni, nie podejmowały działań w celu wdrożenia systemu służącego weryfikacji oraz poprawie rozwiązań z zakresu bezpieczeństwa teleinformatycznego.** Podmioty państwowe nie były organizatorem ćwiczeń dotyczących bezpieczeństwa cyberprzestrzeni i incydentalnie uczestniczyły w tego typu wydarzeniach organizowanych przez instytucje pozarządowe oraz organizacje międzynarodowe. ABW oraz NASK przeprowadzały testy i audyty mające na celu sprawdzenie poprawności rozwiązań z zakresu bezpieczeństwa teleinformatycznego,

natomiast działalność w tym obszarze nie była w sposób systemowy zaplanowana i podlegała istotnym ograniczeniom wynikającym z nieadekwatnych zasobów (ABW) oraz uwarunkowań biznesowych (NASK).

(szerzej str. 66–67)

12. ABW we współpracy z NASK realizowała projekt dotyczący wytworzenia, utrzymywania i rozbudowy **systemu wczesnego ostrzegania – ARAKIS.GOV.** W ramach ww. przedsięwzięcia, w kilkudziesięciu instytucjach publicznych zainstalowano sondy systemu, dzięki którym **uzyskiwano informacje o zagrożeniach w sieci Internet.** Ze względu na braki finansowe, dobrowolność udziału w projekcie oraz instalowanie sond wyłącznie w podmiotach publicznych, **zasięg oddziaływania systemu ARAKIS.GOV oraz pozyskiwanych za jego pomocą danych miały ograniczony zakres. Jednocześnie nie zostały podjęte żadne działania systemowe, mające na celu budowę ogólnokrajowego systemu wczesnego ostrzegania. Minister Administracji i Cyfryzacji nie dysponował wiedzą na temat systemu ARAKIS.GOV oraz nie występował z inicjatywą rozbudowy narzędzi służących do monitorowania zdarzeń w sieci Internet.**

(szerzej str. 68–69)

13. **Nie wypracowano dotychczas założeń systemu działań edukacyjnych, skierowanych do różnych grup administratorów i użytkowników cyberprzestrzeni, mającego na celu podnoszenie kwalifikacji w zakresie bezpieczeństwa teleinformatycznego oraz zwiększanie świadomości zagrożeń występujących w Internecie.** Kierownictwo podmiotów państwowych, w tym w szczególności Minister Administracji i Cyfryzacji, nie planowało i nie prowadziło zorganizowanych szkoleń pracowników administracji publicznej dotyczących bezpieczeństwa IT. Nie podejmowano również działań w celu wypracowania alternatywnego systemu zachęt, który przy uwzględnieniu istniejących ograniczeń finansowych, pozwoliłby instytucjom państwowym pozyskiwać i utrzymywać wysokiej klasy specjalistów do spraw ochrony cyberprzestrzeni. **Poza oddolnymi inicjatywami podmiotów, takich jak NASK, Policja, czy RCB nie były prowadzone systemowe działania, mające na celu edukowanie obywateli w zakresie zagrożeń związanych z korzystaniem z Internetu i możliwych metod zabezpieczenia przed nimi. Obowiązujące w tym zakresie przepisy Prawa telekomunikacyjnego były wadliwie skonstruowane i niewykorzystywane w praktyce.**

(szerzej str. 69–71)

14. **Nie zostało dotychczas wypracowane zintegrowane i systemowe podejście dotyczące wspierania przez państwo badań i rozwoju w obszarze ochrony cyberprzestrzeni oraz możliwości praktycznego zastosowania ich wyników w celu poprawy bezpieczeństwa teleinformatycznego.** W okresie objętym kontrolą, realizowano przy udziale środków publicznych, pojedyncze projekty naukowo-badawcze związane z ochroną cyberprzestrzeni. Były to jednak **przedsięwzięcia niespójne programowo, ukierunkowane przede wszystkim na realizację interesów beneficjentów projektów.** Szczegółowa analiza wyników 5 projektów naukowo-badawczych, na których realizację wydatkowano dotychczas łączną kwotę 17,3 mln zł wykazała, że **nie miały one praktycznego zastosowania w realizacji zadań dotyczących bezpieczeństwa teleinformatycznego państwa.** Znaczna część objętych kontrolą podmiotów państwowych, w tym w szczególności Minister Administracji i Cyfryzacji, nie inicjowała i nie uczestniczyła w wypracowaniu założeń projektów naukowo-badawczych związanych z ochroną cyberprzestrzeni.

(szerzej str. 71–72)

2.3 Uwagi i wnioski

W ocenie NIK, ustalenia niniejszej kontroli wskazują na konieczność bezzwłocznego podjęcia skoordynowanych, systemowych działań prowadzących do wdrożenia realnych mechanizmów ochrony cyberprzestrzeni RP. W celu wyeliminowania najpoważniejszej przeszkody, która sparaliżowała aktywność państwa w tym zakresie w latach 2008–2014, tj. sprzecznych interesów poszczególnych instytucji publicznych, konieczne jest bezpośrednie zaangażowanie w realizację tych zadań najwyższego kierownictwa administracji rządowej – Rady Ministrów i Prezesa Rady Ministrów. Kolejnymi warunkami efektywnej ochrony cyberprzestrzeni, jest wdrożenie mechanizmów współpracy podmiotów prywatnych i państwowych oraz zapewnienie odpowiedniego finansowania działań związanych z bezpieczeństwem IT.

W opinii NIK, najważniejsze działania naprawcze, umożliwiające stworzenie i skuteczne funkcjonowanie krajowego systemu ochrony cyberprzestrzeni powinny obejmować:

1. **Ukierunkowanie działań państwa związanych z utrzymaniem bezpieczeństwa cyberprzestrzeni przede wszystkim na infrastrukturę krytyczną.** W pierwszej kolejności należy zmodyfikować istniejące obecnie kryteria identyfikacji infrastruktury krytycznej tak, aby pozwalały one na pełną i skuteczną inwentaryzację komponentów teleinformatycznych. W ocenie NIK, należy również rozważyć zmianę obecnie funkcjonującego modelu, w którym identyfikacja infrastruktury krytycznej jest prowadzona przez ministrów i kierowników urzędów centralnych, a RCB zasadniczo ogranicza się do uporządkowania i agregacji otrzymanych informacji. Zasadne wydaje się przypisanie tych zadań wyspecjalizowanemu organowi, który posługując się obiektywnymi kryteriami i właściwą metodyką będzie aktywnie zbierał z wielu źródeł i weryfikował informacje pozwalające na identyfikację infrastruktury kluczowej dla funkcjonowania państwa.
2. **Włączenie procesu szacowania ryzyka dotyczącego cyberprzestrzeni w realizowany już proces analizy ryzyka związany z bezpieczeństwem infrastruktury krytycznej,** którego przebieg powinien zostać zdecydowanie usprawniony oraz zaopatrzony w odpowiednie wytyczne i instrukcje określające wymagania, co do treści i jakości wszystkich jego elementów. Należycie przeprowadzona analiza ryzyka w obiektywny sposób wskaże kierunki działań związanych z bezpieczeństwem teleinformatycznym państwa.
3. **Dokonanie dyslokacji ograniczonych zasobów budżetu przeznaczanych obecnie na różne aspekty bezpieczeństwa państwa**, adekwatnie do wyników opisanej powyżej analizy ryzyka.

Niezbędne jest także:

- **przyjęcie przez Radę Ministrów narodowej strategii zarządzania zagrożeniami występującymi w cyberprzestrzeni** określającej: cele i strukturę organizacyjną krajowego systemu ochrony cyberprzestrzeni, zadania poszczególnych jego uczestników i przypisane do nich, precyzyjnie zdefiniowane produkty, mierniki i terminy realizacji;
- **określenie systemu finansowania zadań związanych z ochroną cyberprzestrzeni;**
- **przyjęcie ram prawnych krajowego systemu ochrony cyberprzestrzeni**, poprzez uchwalenie odrębnej ustawy określającej obowiązki oraz uprawnienia poszczególnych państwowych i prywatnych podmiotów realizujących zadania w zakresie bezpieczeństwa teleinformatycznego. Konieczne jest również dokonanie inwentaryzacji i nowelizacji istniejących obecnie regulacji

prawnych dotyczących m.in. zarządzania kryzysowego, Prawa telekomunikacyjnego, informatyzacji, tak aby mogły być one skutecznie wykorzystywane w celu ochrony infrastruktury teleinformatycznej państwa;

- **wyznaczenie krajowego organu koordynującego działania innych podmiotów w zakresie ochrony cyberprzestrzeni, będącego jednocześnie CERTem narodowym**. Zadania ww. organu powinny w szczególności obejmować: koordynację działań w przypadku cyberataku, współpracę z partnerami zagranicznymi oraz użytkownikami i administratorami cyberprzestrzeni spoza infrastruktury krytycznej, wymianę informacji na temat zagrożeń z podmiotami państwowymi i prywatnymi, monitorowanie zagrożeń i wydawanie ostrzeżeń, przygotowanie procesu szacowania ryzyka i agregację jego wyników, organizację narodowych ćwiczeń i testów w zakresie cyberbezpieczeństwa, inwentaryzację kluczowych, krajowych zasobów IT. **W celu skutecznej realizacji tych zadań konieczne jest wyposażenie krajowego organu koordynującego w odpowiednie zasoby techniczne, finansowe i ludzkie oraz nadanie mu ustawowych uprawnień w zakresie żądania informacji od podmiotów prywatnych i państwowych, a także wydawania im wiążących wytycznych**[9]. W opinii NIK, należy rozważyć przypisanie zadań krajowego organu koordynującego ochronę cyberprzestrzeni – Rządowemu Centrum Bezpieczeństwa. Powyższe wynika zarówno z faktu, że RCB jest podmiotem mającym doświadczenie w zakresie identyfikowania infrastruktury krytycznej, szacowania ryzyka i reagowania na sytuacje kryzysowe, jak i z analiz wskazujących, że incydenty teleinformatyczne stanowią obecnie jedno z najbardziej powszechnych zagrożeń infrastruktury państwa. Alternatywna propozycja została przedstawiona w opracowaniu przygotowanym dla NIK przez ekspertów zewnętrznych[10], w którym zawarto postulat utworzenia nowego organu odpowiadającego za bezpieczeństwo teleinformatyczne – Narodowego Centrum Cyberbezpieczeństwa;
- **wdrożenie krajowego systemu reagowania na incydenty komputerowe**. W opinii NIK, budowa ww. systemu powinna obejmować w szczególności:
  - **ustanowienie obowiązków w zakresie raportowania o incydentach**, obejmujących co najmniej podmioty zarządzające infrastrukturą krytyczną, przedsiębiorców telekomunikacyjnych i podmioty administracji państwowej (w tym samorządowej);
  - ustanowienie kanałów wymiany informacji między różnymi rządowymi, cywilnymi i wojskowymi zespołami reagowania oraz klasyfikacji incydentów i przypisanych do niej procedur działania;
  - rozbudowę zespołów CERT;
- **ustanowienie podstawowych wymogów w zakresie bezpieczeństwa cyberprzestrzeni.** Zdaniem NIK, powinny zostać przyjęte minimalne standardy bezpieczeństwa IT – obowiązujące dla podmiotów zarządzających infrastrukturą krytyczną i całej administracji państwowej. Wytyczne w ww. zakresie powinny być również formułowane dla pozostałych użytkowników cyberprzestrzeni (mniejsze firmy, osoby prywatne);

[9] Brak zasobów i stosownych uprawnień, były jednymi z ważniejszych przyczyn dotychczasowej, nierzetelnej realizacji zadań w tym zakresie przez Ministra Administracji i Cyfryzacji.

[10] Instytut Kościuszki, „Propozycja modelowych rozwiązań w zakresie budowania cyberbezpieczeństwa Polski", Kraków 2015.

- **opracowanie procedur reagowania kryzysowego i utrzymania ciągłości działania w sytuacji zagrożeń lub zakłócenia działania infrastruktury państwa spowodowanych zdarzeniami występującymi w cyberprzestrzeni;**
- **wdrożenie skoordynowanych, planowych działań administracji państwowej w obszarze podnoszenia kwalifikacji i świadomości różnych grup administratorów i użytkowników cyberprzestrzeni, a także w zakresie wspierania badań i rozwoju dotyczących bezpieczeństwa IT**.

3 WAŻNIEJSZE WYNIKI KONTROLI

3.1 Charakterystyka obszaru objętego kontrolą

Postępujący rozwój społeczeństwa informacyjnego połączony z doskonaleniem i upowszechnianiem rozwiązań informatycznych i telekomunikacyjnych powoduje przenoszenie kolejnych aspektów ludzkiej działalności ze świata rzeczywistego **w cyberprzestrzeń – wirtualny obszar powstały wewnątrz i w zasięgu oddziaływania urządzeń informatycznych oraz telekomunikacyjnych**. Główne cechy cyberprzestrzeni, tj.: globalny zasięg, łatwy dostęp, wydajność, uniwersalność i relatywna „taniość", powodują, że kolejne obszary działalności rządów, firm i osób prywatnych są przenoszone do cyberprzestrzeni. Oprócz takiego transferu obserwujemy również powstawanie, przy wykorzystaniu unikalnych cech cyberprzestrzeni, nieznanych wcześniej form działalności związanych z usługami, wypoczynkiem, produkcją oraz realizacją zadań administracji publicznej. Coraz więcej osób nie wyobraża sobie codziennego funkcjonowania bez korzystania z cyberprzestrzeni: różnorodnych portali, poczty elektronicznej, komunikatorów, cyfrowych bibliotek, powszechnej łączności bezprzewodowej oraz wirtualnych pieniędzy. Dostęp do tego równoległego świata w ciągu niewielu lat awansował z poziomu akademickiego eksperymentu do podstawowego medium, równie istotnego jak bieżąca woda, energia elektryczna, czy gaz. Ten nieskrępowany dostęp stał się synonimem wolności obywatelskiej – wypowiadania się i wymiany poglądów bez jakiejkolwiek instytucjonalnej kontroli – pozwalając na dokonywanie zmian społecznych, obalanie rządów, organizowanie protestów, omijanie niesprawiedliwych, w ocenie niektórych grup, systemów dystrybucji dóbr i towarów. Rosnący stopień wykorzystania cyberprzestrzeni przez biznes, instytucje rządowe i administrację publiczną spowodował oprócz oferowania nowej jakości towarów i usług stopniowe uzależnianie ich dostępności od sprawnego funkcjonowania systemów informatycznych i łączności. Od wielu z tych zmian nie ma możliwości odwrotu. Nowe usługi i towary stały się powszechne, a dotychczasowe metody ich świadczenia i dostarczania – przestarzałe oraz nieopłacalne.

Niestety, do cyberprzestrzeni przeniknęły również negatywne zjawiska typowe dla świata rzeczywistego. Wszystkie cechy, które zadecydowały o powstaniu nowej jakości w komunikacji, handlu, czy usługach stały się również okolicznością sprzyjającą powstawaniu zupełnie nowych możliwości dla chuliganów, złodziei, terrorystów, czy szpiegów. Poczucie anonimowości, brak geograficznych granic, łatwość ukrywania i szyfrowania treści, ogromna prędkość zmian technicznych sprzyjająca wykorzystywaniu wynikających z niej ludzkich błędów i pomyłek powodują, że zagrożenia płynące z tej strony stają się coraz poważniejsze.

Cyberprzestrzeń utworzona przed wielu laty, jako narzędzie pracy dla garstki naukowców, w wyniku dynamicznego rozwoju osiągnęła obecny globalny i wszechstronny charakter. Odbyło się to praktycznie bez nadzoru i współpracy instytucji państwowych. Wiele krajów (z pominięciem jedynie tych o totalitarnym systemie władzy), potraktowało rozwój cyberprzestrzeni analogicznie do istniejących już wcześniej rynków łączności telefonicznej i mediów, pozostawiając praktycznie cały jej rozwój, nadzór i kontrolę w rękach firm prywatnych. Obecną konsekwencją tej decyzji (lub może zaniechania) jest dotycząca praktycznie wszystkich krajów demokratycznych sytuacja, w której rząd i administracja państwowa nie posiadają mechanizmów pozwalających na nadzorowanie i regulowanie funkcjonowania cyberprzestrzeni wykorzystywanej przez podmioty i obywateli z danego kraju. Dodatkowym utrudnieniem jest globalny charakter cyberprzestrzeni, w której podziały biegną, nie według granic państwowych, czy administracyjnych, ale według zasięgu: rynków, usług, technologii oraz języka. Dynamika zmian zachodzących w cyberprzestrzeni,

ich innowacyjność i powiązanie z najnowocześniejszymi technologiami powoduje powstawanie luki prawnej – istotnego zakresu działalności niosącej skutki prawne i ekonomiczne nieuwzględnionego w pełni w systemach prawnych, tak krajowych, jak i międzynarodowych. Zupełnie nowym zjawiskiem jest rozwijająca się obecnie gwałtownie „cyberprzestrzeń przedmiotów", w której wymiana informacji nie jest prowadzona pomiędzy ludźmi, ale pomiędzy przedmiotami (urządzeniami). Tego rodzaju dialog obejmujący stopniowo telewizory, lodówki, samochody, inteligentne budynki, maszyny i urządzenia a nawet silniki w lecących samolotach, odbywający się praktycznie bez świadomości użytkowników, poza ułatwieniami w eksploatacji i zmniejszeniem np. kosztów serwisu, staje się również źródłem rosnącego zagrożenia.

Źródła zagrożeń w cyberprzestrzeni

Podstawowy podział zagrożeń występujących w cyberprzestrzeni związany jest z celami, jakie przyświecają pojedynczym ludziom, czy też organizacjom. Według tego kryterium można wyodrębnić następujące zagrożenia:

1. **Cyber-chuligani** – pojedyncze osoby lub niewielkie grupy prowadzące działania w celu sprawdzenia lub udowodnienia swoich umiejętności, dokonania odwetu, na przykład na adwersarzu lub byłym pracodawcy.
2. **Cyber-aktywiści** – grupy osób prowadzące działania w celu wsparcia jakiejś idei, dążące do jej rozpowszechnienia za pomocą spektakularnych działań o dużym zasięgu i zakresie, które mają godzić w czyjś wizerunek. Działania takie nie powinny, w mniemaniu atakujących, powodować istotnych strat finansowych.
3. **Cyber-przestępcy** – pojedyncze osoby lub grupy osób prowadzące działania w celu uzyskania korzyści materialnej, dokonujące przeważnie klasycznego oszustwa lub wyłudzenia z wykorzystaniem środków, metod i narzędzi dostępnych w cyberprzestrzeni.
4. **Cyber-terroryści** – pojedyncze osoby, grupy osób lub organizacje polityczne prowadzące działania w cyberprzestrzeni dla wsparcia swoich celów politycznych, dążące do ich osiągnięcia poprzez zastraszenie i wywołanie stanu zagrożenia. Wykorzystujące również cyberprzestrzeń, jako narzędzie komunikacji, propagandy, gromadzenia środków finansowych oraz werbunku i szkolenia.
5. **Cyber-szpiedzy** – organizacje lub firmy pracujące na rzecz biznesu lub resortów siłowych prowadzące działania w cyberprzestrzeni w celu skrytego pozyskania wiedzy lub wywarcia wpływu. Wiele państw (w tym szczególnie Chiny, USA, czy też Rosja) na szeroką skalę wykorzystują cyberprzestrzeń do zbierania informacji szczególnie gospodarczych i technologicznych. Jest to niezwykle tania, efektywna i łatwa do ukrycia forma działalności wywiadowczej.
6. **Cyber-żołnierze** – organizacje najemnicze lub oddziały wojskowe przeznaczone do prowadzenia działań zbrojnych w cyberprzestrzeni traktowanej jako kolejny teatr działań wojennych. Mogą być one prowadzone samodzielnie lub we współpracy z innymi rodzajami sił zbrojnych.

Należy podkreślić, że powyższy podział ma jedynie charakter umowny, a w wielu wypadkach jednoznaczne zakwalifikowanie źródeł zagrożeń jest utrudnione lub niemożliwe, co wynika m.in. z celowych zabiegów atakującego lub błędów w przeprowadzonej analizie.

Do najpopularniejszych zagrożeń w cyberprzestrzeni należą:

1. Użycie szkodliwego oprogramowania (wirusy, robaki, konie trojańskie, tylne wejścia, programy szpiegujące, procedury wykorzystujące znane lub ukrywane luki w programach komercyjnych).
2. Kradzież i wykorzystywanie cudzych danych osobowych.
3. Wyłudzanie, kradzież, fałszowanie lub niszczenie danych.
4. Blokowanie dostępu do usług (bomby pocztowe, przeciążanie aplikacji i serwisów, masowe zawłaszczanie systemów komputerowych w celu wykorzystywania ich do prowadzenia takich przeciążeń).
5. Przesyłanie niepotrzebnej lub niechcianej informacji.
6. Ataki socjotechniczne (wyłudzanie informacji poprzez podszywanie się pod instytucję lub osobę zaufaną).
7. Zaawansowane ataki celowane (prowadzone za pomocą wielu skoordynowanych i zindywidualizowanych metod ataki skierowane precyzyjnie przeciwko konkretnej osobie, organizacji lub firmie).

Zagrożenia dotyczące Polski

Przyśpieszony w ciągu ostatnich kilkunastu lat postęp, jaki nastąpił w poziomie życia Polaków i w funkcjonowaniu polskiej gospodarki spowodował, że technologiczna luka, która przez dziesięciolecia odgradzała nas od światowego postępu i chroniła przed związanymi z nim zagrożeniami zaczęła się szybko kurczyć. Polska cyberprzestrzeń jest faktem. Korzystają z jej możliwości Polacy, polskie firmy, rząd i administracja publiczna. Jednocześnie będąc elementem cyberprzestrzeni globalnej umożliwia ona nieskrępowany dostęp dla podmiotów zagranicznych. Faktem jest również rosnąca liczba ataków znajdujących swoje odzwierciedlenie w informacjach medialnych. Ataki wymierzone w styczniu 2012 r. w najważniejsze strony internetowe administracji publicznej w domenie gov.pl stały się fragmentem kampanii protestu społecznego związanej z pracami, mającymi na celu podpisanie przez Polskę międzynarodowego porozumienia dotyczącego walki z naruszaniem własności intelektualnej (**tzw. ACTA**). Ataki dotyczyły stron internetowych Kancelarii Sejmu RP, Kancelarii Prezydenta RP, Kancelarii Prezesa Rady Ministrów, Ministerstwa Spraw Zagranicznych, Ministerstwa Sprawiedliwości, Ministerstwa Edukacji Narodowej, Kancelarii Senatu RP, Ministerstwa Kultury i Dziedzictwa Narodowego, Ministerstwa Obrony Narodowej, Komendy Głównej Policji oraz Centralnego Biura Antykorupcyjnego. Ich celem było przeciążenie serwerów udostepniających strony WWW tych instytucji. Z przeprowadzonych analiz wynika, że przeważająca większość ruchu związanego z tym atakiem pochodziła z polskich adresów IP. Kolejnym istotnym incydentem było **wykradzenie i opublikowanie w Internecie danych z serwerów Ministerstwa Gospodarki**. Wykradzione dokumenty, (w większości o mało istotnej treści), zawierały kopie stron paszportów (głównie obcokrajowców, np. zapraszanych do Polski w sprawach handlu przez Wydział Promocji Handlu i Inwestycji Ambasady Rzeczypospolitej Polskiej w Republice Białorusi), dane skrzynek pocztowych wraz z brzmieniem ich haseł oraz obrazy rządowych dokumentów. Oba powyższe incydenty pomimo tego, że nie spowodowały istotnych strat (poza wizerunkowymi) były powodem doraźnego podjęcia przez administrację rządową szeregu działań zabezpieczających.

W trakcie trwania niniejszej kontroli dwukrotnie, w lipcu i październiku 2014 r., miały miejsce w Polsce **cyberataki o charakterze terrorystycznym**. Anonimowi nadawcy, posługując się

narzędziami informatycznymi uniemożliwiającymi identyfikację, przesłali za pomocą Internetu wiadomości ostrzegające o podłożeniu ładunków wybuchowych w siedzibach wielu instytucji. Dzisiaj wiadomo, że informacje te były nieprawdziwe, co nie zmienia jednak ich terrorystycznego charakteru oraz odpowiedzialności za koszty akcji ewakuacyjnych i utrudnień w funkcjonowaniu instytucji.

W październiku 2014 r. miała także miejsce kradzież danych z systemów informatycznych Giełdy Papierów Wartościowych (GPW). Wykradzione dane osobowe oraz wrażliwe informacje dotyczące funkcjonowania systemów informatycznych GPW zostały przez złodziei anonimowo upublicznione w Internecie wraz z informacją o politycznych i międzynarodowych pobudkach ich kradzieży. Opublikowane informacje techniczne umożliwiły przeprowadzenie włamań do kolejnych systemów wykorzystywanych przez klientów GPW.

W listopadzie 2014 r. wykradziono z systemu informatycznego dane dotyczące pracowników Państwowej Komisji Wyborczej. Miało to miejsce w czasie, kiedy Komisja borykała się z błędami w oprogramowaniu służącym do obliczenia wyników przeprowadzonych wyborów.

Opisane powyżej zdarzenia, które uzyskały duży rozgłos medialny nie wyczerpują listy incydentów, jakie ostatnio dotyczyły użytkowników polskiej cyberprzestrzeni, i tak np.:

- w listopadzie 2013 r. udostępniono w Internecie dane osobowe 400 000 abonentów firmy telekomunikacyjnej Hyperion z Katowic;
- w grudniu 2013 r. zaoferowano w sieci dane setek tysięcy abonentów operatora telekomunikacyjnego Orange: imiona i nazwiska, nr telefonów, PESEL, NIP i dokumentów tożsamości oraz adresy tradycyjne i e-mail;
- polscy użytkownicy, w tym również pracownicy administracji państwowej, padają także ofiarami incydentów dotyczących firm obcych (zagranicznych), z których powierzone im dane zostały skradzione lub skopiowane.

Nieznana pozostaje skala ataków, w przypadku których nie ujawniono informacji o ich skutecznym przeprowadzeniu – niejednokrotnie ofiary takich ataków, ze względów wizerunkowych, nie są zainteresowane udostępnianiem tych informacji.

Rola administracji państwowej

Wątpliwości może budzić rola administracji państwowej w zwalczaniu zagrożeń w cyberprzestrzeni. Czy w sytuacji, gdy przeważająca większość infrastruktury obsługującej polską cyberprzestrzeń jest w rękach podmiotów komercyjnych (głównie prywatnych) dysponujących unikalną wiedzą i przygotowanymi pracownikami, istnieje możliwość i potrzeba podejmowania przez państwo skutecznych działań dla podwyższenia bezpieczeństwa? Wydaje się, że tak. **Koniecznym jest budowanie adekwatnego do zachodzących przemian systemu prawnego, pozwalającego na powszechne wdrożenie i egzekwowanie właściwych zasad i praktyk, gwarantującego utrzymanie przez wszystkich kluczowych administratorów oraz użytkowników cyberprzestrzeni niezbędnego i spójnego poziomu bezpieczeństwa, normalizującego procesy i procedury związane z szacowaniem ryzyka, profilaktyką, obroną przed atakami oraz minimalizowaniem ich skutków. Koniecznym jest również podjęcie przez państwo roli koordynatora i łącznika organizującego współpracę i wymianę informacji pomiędzy wszystkimi podmiotami zagrożonymi atakami i podejmującymi działania obronne oraz stworzenie kanałów dystrybucji informacji dotyczących ewentualnych zagrożeń uzyskiwanych przez państwo metodami niedostępnymi dla podmiotów komercyjnych**

(dyplomacja, wywiad, kontrwywiad i współpraca międzynarodowa). Zasadność przedstawionego powyżej podejścia potwierdza fakt intensyfikowania w minionych latach działań w zakresie ochrony cyberprzestrzeni przez rządy takich państw jak np. USA, Wielka Brytania, Niemcy, czy Łotwa (kraje nadbałtyckie były kilkakrotnie celem ataków o znaczącej dla nich skali).

Pojęcie **„cyberprzestrzeni"** zostało wprowadzone do polskiego systemu prawnego na podstawie ustawy z dnia 30 sierpnia 2011 r. o zmianie ustawy o stanie wojennym oraz o kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej oraz niektórych innych ustaw[11]. **Zgodnie z ww. definicją, przez cyberprzestrzeń należy rozumieć przestrzeń przetwarzania i wymiany informacji tworzoną przez systemy teleinformatyczne[12] wraz z powiązaniami między nimi oraz relacjami z użytkownikami. Zagrożenia państwa związane z działaniami występującymi w cyberprzestrzeni zostały uznane za jedną z przesłanek wprowadzenia, wymienionych w art. 228 ust. 1 Konstytucji RP[13], stanów nadzwyczajnych, tj. stanu wojennego, stanu wyjątkowego lub stanu klęski żywiołowej**[14].

Obowiązki związane z ochroną cyberprzestrzeni spoczywają w pierwszej kolejności na podmiotach komercyjnych, co wynika z faktu, że kontrolują one przeważającą część krajowych systemów i sieci teleinformatycznych oraz realizują za ich pośrednictwem usługi i transakcje handlowe. Przykładowymi regulacjami nakładającymi obowiązki w ww. zakresie są:

- art. 175 oraz art. 175c ust. 1 pkt 1-2 ustawy z dnia 16 lipca 2004 r. Prawo telekomunikacyjne[15], na podstawie których przedsiębiorcy telekomunikacyjni są zobowiązani podejmować środki techniczne i organizacyjne w celu zapewnienia bezpieczeństwa i integralności sieci, usług oraz przekazu komunikatów (obejmujące m.in. eliminację przekazu, który zagraża bezpieczeństwu sieci lub usług oraz przerwanie świadczenia usługi telekomunikacyjnej na zakończeniu sieci, z którego następuje wysyłanie komunikatów zagrażających bezpieczeństwu) oraz informować użytkowników o wystąpieniu ryzyka naruszenia bezpieczeństwa, a także o istniejących możliwościach zapewnienia bezpieczeństwa. Na podstawie art. 176a ust. 2 ww. ustawy przedsiębiorcy telekomunikacyjni zostali również zobowiązani do posiadania aktualnych, opracowanych w uzgodnieniu z właściwymi organami państwowymi, planów działania w sytuacjach szczególnych zagrożeń;
- art. 7 pkt 1 ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną[16], zgodnie z którym usługodawcy są zobowiązani zapewnić korzystanie z usługi świadczonej drogą elektroniczną w sposób uniemożliwiający dostęp osób nieuprawnionych do treści przekazu

[11] Dz. U. Nr 222, poz. 1323. Przedmiotowa definicja została wprowadzona do trzech ustaw, tj.: ustawy z dnia 29 sierpnia 2002 r. o stanie wojennym oraz o kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej (Dz. U. z 2014 r., poz. 1815.), ustawy z dnia 21 czerwca 2002 r. o stanie wyjątkowym (Dz. U. z 2014 r., poz. 1191.), ustawy z dnia 18 kwietnia 2002 r. o stanie klęski żywiołowej (Dz. U. z 2014 r., poz. 333 ze zm.).

[12] Na podstawie art. 3 pkt 3 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2014 r., poz. 1114), „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.

[13] Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. (Dz. U. Nr 78, poz. 483 ze zm.)

[14] Art. 2 ust. 1 ustawy o stanie wojennym oraz o kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej, art. 2 ust. 1 ustawy o stanie wyjątkowym, art. 2 ustawy o stanie klęski żywiołowej.

[15] Dz. U. z 2014 r., poz. 243 ze zm.

[16] Dz. U. z 2013 r., poz. 1422.

składającego się na tę usługę oraz jednoznaczną identyfikację stron usługi i potwierdzenie faktu złożenia oświadczeń woli niezbędnych do zawarcia drogą elektroniczną umowy;

- art. 50 ust. 2 ustawy z dnia 29 sierpnia 1997 r. Prawo bankowe[17], na podstawie którego banki powinny dokładać szczególnej staranności w zakresie zapewnienia bezpieczeństwa przechowywanych środków pieniężnych;
- art. 10 ust 1 pkt 3 oraz art. 10 ust. 2 ustawy z dnia 18 września 2001 r. o podpisie elektronicznym[18] nakładający na podmioty świadczące usługi certyfikacyjne związane z podpisem elektronicznym obowiązek zapewnienia środków przeciwdziałających fałszerstwom certyfikatów i innych danych poświadczanych elektronicznie przez te podmioty, w szczególności przez ochronę urządzeń i danych wykorzystywanych przy świadczeniu usług certyfikacyjnych.

Dotychczas nie zostały przyjęte akty normatywne definiujące w sposób jednolity, spójny i precyzyjny katalog podmiotów państwowych odpowiadających za ochronę cyberprzestrzeni RP oraz określające ich zadania. Nie oznacza to jednak, że obszar ten jest zupełnie nieuregulowany. **Czynności związane z ochroną cyberprzestrzeni powinny być realizowane przez różne podmioty i jednostki państwowe na podstawie ogólnych regulacji prawnych określających ich zadania i kompetencje. Podmiotami tymi są w szczególności:**

1. **Rada Ministrów** – na podstawie art. 146 ust. 4 pkt 7 i 11 Konstytucji RP – zapewnia bezpieczeństwo wewnętrzne państwa i porządek publiczny oraz sprawuje ogólne kierownictwo w dziedzinie obronności kraju.
2. **Minister Administracji i Cyfryzacji** – zgodnie z § 1 ust. 2 pkt 1-3 rozporządzenia Prezesa Rady Ministrów z dnia 22 września 2014 r. w sprawie szczegółowego zakresu działania Ministra Administracji i Cyfryzacji[19] – kieruje działami administracji rządowej administracja publiczna, informatyzacja i łączność. Dział administracja publiczna obejmuje m.in. przeciwdziałanie i usuwanie skutków klęsk żywiołowych i innych podobnych zdarzeń zagrażających bezpieczeństwu powszechnemu (art. 6 ust. 1 ustawy z dnia 4 września 1997 r. o działach administracji rządowej[20]), dział informatyzacja obejmuje w szczególności sprawy: informatyzacji administracji publicznej, systemów i sieci teleinformatycznych administracji publicznej, standardów informatycznych, zastosowań technologii informatycznych w społeczeństwie informacyjnym, rozwoju usług świadczonych drogą elektroniczną, realizacji zobowiązań międzynarodowych w dziedzinie informatyzacji, koordynacji interoperacyjności (art. 12a ww. ustawy), dział łączność obejmuje w szczególności sprawy telekomunikacji (art. 16 ust. 1 ww. ustawy).
3. **Minister Spraw Wewnętrznych** – zgodnie z § 1 ust. 2 rozporządzenia Prezesa Rady Ministrów z dnia 22 września 2014 r. w sprawie szczegółowego zakresu działania Ministra Spraw Wewnętrznych[21] – kieruje działem administracji rządowej sprawy wewnętrzne obejmującym m.in. sprawy ochrony bezpieczeństwa i porządku publicznego oraz zarządzania kryzysowego[22].

17 Dz. U. z 2015 r., poz. 128.
18 Dz. U. z 2013 r., poz. 262 ze zm.
19 Dz. U. z 2014 r., poz. 1254.
20 Dz. U. Nr 2013 r., poz. 743 ze zm.
21 Dz. U. z 2014 r., poz. 1265.
22 Art. 29 ust. 1 pkt 1 i 3 ustawy o działach administracji rządowej.

4. **Agencja Bezpieczeństwa Wewnętrznego** (ABW) – na podstawie art. 5 ust. 1 pkt 1 – 4 ustawy z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu[23] do zadań ABW należy m.in. rozpoznawanie, zapobieganie i zwalczanie zagrożeń godzących w bezpieczeństwo wewnętrzne państwa, rozpoznawanie, zapobieganie i wykrywanie przestępstw szpiegostwa, terroryzmu, bezprawnego ujawnienia lub wykorzystania informacji niejawnych i innych przestępstw godzących w bezpieczeństwo oraz w podstawy ekonomiczne państwa, uzyskiwanie, analizowanie, przetwarzanie i przekazywanie właściwym organom informacji mogących mieć istotne znaczenie dla ochrony bezpieczeństwa wewnętrznego państwa.

   Na podstawie wspólnego stanowiska Kierownictwa MSWiA i ABW ze stycznia 2008 r., w ramach ABW został powołany **Rządowy Zespół Reagowania na Incydenty Komputerowe CERT.GOV.PL**, do którego zadań należy zapewnianie i rozwijanie zdolności jednostek organizacyjnych administracji publicznej do ochrony przed zagrożeniami, ze szczególnym uwzględnieniem ataków ukierunkowanych na infrastrukturę obejmującą systemy i sieci teleinformatyczne, których zniszczenie lub zakłócenie może stanowić zagrożenie dla życia, zdrowia ludzi, dziedzictwa narodowego oraz środowiska w znacznych rozmiarach, albo spowodować poważne straty materialne, a także zakłócić funkcjonowanie państwa[24].

5. **Minister Obrony Narodowej** – zgodnie z rozporządzeniem Rady Ministrów z dnia 9 lipca 1996 r. w sprawie szczegółowego zakresu działania Ministra Obrony Narodowej[25] – odpowiada m.in. za: gromadzenie informacji oraz prowadzenie analiz i opracowywanie prognoz kształtowania się warunków bezpieczeństwa państwa, przygotowywanie projektów dokumentów strategicznych w zakresie polityki obronnej oraz planów obrony państwa, koordynowanie przygotowań organów administracji rządowej, organów jednostek samorządu terytorialnego, instytucji państwowych, przedsiębiorców i innych podmiotów do funkcjonowania w okresie zewnętrznego zagrożenia bezpieczeństwa państwa i w czasie wojny (§ 1 pkt 1 lit. a i b oraz § 1 pkt 3 lit. b ww. rozporządzenia).

   W resorcie obrony narodowej zorganizowano trzypoziomowy system reagowania na incydenty komputerowe (SRnIK) złożony z Centrum Koordynacyjnego, Centrum Technicznego oraz administratorów systemów i sieci teleinformatycznych w jednostkach i komórkach organizacyjnych resortu[26]. W ramach Centrum Technicznego funkcjonuje zespół reagowania na incydenty komputerowe **MIL-CERT.PL**, odpowiadający za obsługę zdarzeń występujących w resortowych sieciach informatycznych. Ponadto powołany został **Pełnomocnik Ministra Obrony Narodowej ds. Bezpieczeństwa Cyberprzestrzeni**[27], do którego zadań należy m.in.: koordynowanie przedsięwzięć przewidzianych dla Ministra w sprawach bezpieczeństwa cyberprzestrzeni, inicjowanie oraz wspieranie działań w obszarze osiągania zdolności do zapewnienia bezpieczeństwa cyberprzestrzeni resortu obrony narodowej, sprawowanie nadzoru nad realizacją zadań wynikających z aktów prawnych, polityk i programów rządowych dotyczących zapewnienia bezpieczeństwa cyberprzestrzeni.

---

23 Dz. U. z 2010 r. Nr 29, poz. 154 ze zm.

24 Zob. m.in.: http://www.cert.gov.pl/cer/o-nas/15,O-nas.html.

25 Dz. U. Nr 94, poz. 426 ze zm.

26 Decyzja Nr 243/MON Ministra Obrony Narodowej z dnia 18 czerwca 2014 r. w sprawie organizacji i funkcjonowania systemu reagowania na incydenty komputerowe w resorcie obrony narodowej (Dz. Urz. MON z 2014 r., poz. 203.).

27 Decyzja Nr 38/MON Ministra Obrony Narodowej z dnia 16 lutego 2012 r. w sprawie powołania Pełnomocnika Ministra Obrony Narodowej ds. Bezpieczeństwa Cyberprzestrzeni (Dz. Urz. MON z 2012 r., poz., 52 ze zm.).

Struktury MON dedykowane do realizacji zadań związanych z ochroną cyberprzestrzeni podlegają dalszej rozbudowie. W 2010 r. utworzono Centrum Bezpieczeństwa Cybernetycznego Sił Zbrojnych[28], a z dniem 1 czerwca 2013 r. państwową jednostkę budżetową podległą Ministrowi Obrony Narodowej – Narodowe Centrum Kryptologii[29].

6. **Policja** – zgodnie z art. 1 ust. 2 pkt 1–3 ustawy z dnia 6 kwietnia 1990 r. o Policji[30] do zadań tej formacji należy m.in.: ochrona życia i zdrowia ludzi oraz mienia przed bezprawnymi zamachami naruszającymi te dobra, ochrona bezpieczeństwa i porządku publicznego, inicjowanie i organizowanie działań mających na celu zapobieganie popełnianiu przestępstw i wykroczeń oraz zjawiskom kryminogennym. W Komendzie Głównej Policji, zadania związane z nadzorowaniem i koordynowaniem przedsięwzięć wspierających zwalczenie cyberprzestępczości realizuje Biuro Służby Kryminalnej[31], w ramach którego funkcjonuje Wydział do Walki z Cyberprzestępczością[32].
7. **CERT Polska** jest zespołem reagowania na zdarzenia naruszające bezpieczeństwo w sieci Internet działającym od 1996 r. w strukturach Naukowej i Akademickiej Sieci Komputerowej i finansowanym przez tę instytucję. CERT Polska jest jednym z najważniejszych tego rodzaju zespołów w kraju a jego zakres działania obejmuje domeną internetową „pl." oraz obsługę incydentów występujących w polskich sieciach internetowych. Do głównych zadań zespołu należy: rejestrowanie i obsługa zdarzeń naruszających bezpieczeństwo sieci, alarmowanie użytkowników o zagrożeniach, współpraca z innymi zespołami CERT, prowadzenie działań zmierzających do wzrostu świadomości bezpieczeństwa teleinformatycznego, prowadzenie badań dotyczących bezpieczeństwa Internetu, testowanie produktów z dziedziny bezpieczeństwa teleinformatycznego, prace w zakresie tworzenia wzorców obsługi i rejestracji incydentów[33].

   NASK jest instytutem badawczym utworzonym na podstawie zarządzenia Nr 5/93 Przewodniczącego Komitetu Badań Naukowych z dnia 14 grudnia 1993 r. w sprawie utworzenia jednostki badawczo-rozwojowej pod nazwą Naukowa i Akademicka Sieć Komputerowa, funkcjonującym w oparciu o przepisy ustawy z dnia 30 kwietnia 2010 r. o instytutach badawczych[34]. Działalność Instytutu finansowana jest w przeważającej części z przychodów własnych (uzyskiwanych z działalności komercyjnej) oraz w niewielkim stopniu z dotacji podmiotowych udzielanych przez ministra nadzorującego. Podmiotem sprawującym nadzór nad NASK jest Minister Nauki i Szkolnictwa Wyższego[35], który na podstawie art. 37 ust. 1 ustawy

28 Jednostka utworzona na podstawie decyzji Ministra Obrony Narodowej z dnia 26 kwietnia 2010 r., jako wyspecjalizowana jednostka wojskowa, której głównym zadaniem jest obrona cyberprzestrzeni, poprzez prowadzenie działań w cyberprzestrzeni.

29 Narodowe Centrum Kryptologii zostało utworzone na podstawie zarządzenia Nr 10/MON Ministra Obrony Narodowej z dnia 29 kwietnia 2013 r. w sprawie utworzenia i nadania statutu państwowej jednostce budżetowej - Narodowe Centrum Kryptologii (Dz. Urz. MON z 2013 r., poz. 121 ze zm.).

30 Dz. U. z 2015 r., poz. 355.

31 § 16 ust. 2 pkt 2 zarządzenia Nr 8 Komendanta Głównego Policji z dnia 15 marca 2013 r. w sprawie regulaminu Komendy Głównej Policji (Dz. Urz. KGP z 2013 r., poz. 25 ze zm.).

32 Na podstawie Decyzji Dyrektora BSK KGP z dnia 29 lipca 2014 r. w sprawie szczegółowej struktury organizacyjnej i schematu organizacyjnego Biura Służby Kryminalnej KGP, podziału zadań między dyrektorem a jego zastępcami oraz katalogu zadań komórek organizacyjnych.

33 Zob. min.: http://www.cert.pl/o-nas oraz opis zespołu CERT Polska - http://www.cert.pl/txt/rfc2350.txt .

34 Dz. U. Nr 96, poz. 618 ze zm.

35 Pkt 100 załącznika do obwieszczenia Ministra Nauki i Szkolnictwa Wyższego z dnia 20 stycznia 2014 r. w sprawie wykazu jednostek organizacyjnych podległych Ministrowi Nauki i Szkolnictwa Wyższego lub przez niego nadzorowanych (M.P. z 2014 r., poz. 51).

o instytutach badawczych, może również zlecać tej jednostce realizację zadań niezbędnych ze względu na potrzeby obronności i bezpieczeństwa publicznego, w przypadku klęski żywiołowej lub w celu wykonania zobowiązań międzynarodowych.

8. **Urząd Komunikacji Elektronicznej** (UKE) – zgodnie z art. 175a ust. 1 oraz art. 175c ust. 2 ustawy Prawo telekomunikacyjne, przedsiębiorcy telekomunikacyjni są zobowiązani niezwłocznie informować Prezesa UKE o naruszeniach bezpieczeństwa lub integralności sieci lub usług, które miały istotny wpływ na funkcjonowanie sieci lub usług telekomunikacyjnych oraz o podjętych przez nich działaniach zapobiegawczych i środkach naprawczych. Na podstawie informacji otrzymanych od przedsiębiorców Prezes UKE[36]:
   - informuje o wystąpieniu naruszenia bezpieczeństwa lub integralności sieci lub usług organy regulacyjne innych państw członkowskich UE i ENISA (jeżeli uzna charakter tego naruszenia za istotny) oraz publikuje informacje o zdarzeniu na stronie internetowej UKE lub nakłada na przedsiębiorcę telekomunikacyjnego, w drodze decyzji, obowiązek jej podania do publicznej wiadomości (art. 175b ust. 1 i 2 ww. ustawy);
   - w terminie do końca lutego każdego roku, przekazuje Komisji Europejskiej oraz ENISA sprawozdanie za rok poprzedni zawierające informacje o naruszeniach bezpieczeństwa sieci i usług oraz o działaniach podjętych przez przedsiębiorców telekomunikacyjnych (art. 175b ust. 3 ww. ustawy);
   - w terminie do dnia 30 kwietnia każdego roku opracowuje i przekazuje ministrowi właściwemu do spraw łączności raport o zgłoszonych zagrożeniach i podjętych przez przedsiębiorców telekomunikacyjnych działaniach zapobiegawczych i naprawczych (art. 175b ust. 4 ww. ustawy);
   - publikuje na stronie internetowej UKE aktualne informacje dotyczące m.in.: zagrożeń związanych z korzystaniem przez abonentów z usług telekomunikacyjnych, rekomendowanych środków ostrożności i najbardziej popularnych sposobów zabezpieczania przed oprogramowaniem złośliwym lub szpiegującym, konsekwencji nieodpowiedniego zabezpieczenia telekomunikacyjnych urządzeń końcowych (art. 175e ust. 1 ww. ustawy).

UKE jest również organem uczestniczącym w procesie sporządzania planów działań przedsiębiorców telekomunikacyjnych dotyczących sytuacji kryzysowych, wymaganych na podstawie art. 176a ust. 2 Prawa telekomunikacyjnego. Zgodnie z rozporządzeniem Rady Ministrów z dnia 4 stycznia 2010 r. w sprawie planu działań przedsiębiorcy telekomunikacyjnego w sytuacjach szczególnych zagrożeń[37] przedsiębiorcy sporządzający przedmiotowe plany, dokonują ich uzgodnienia m.in. z Prezesem UKE[38] (§ 8 ust. 1–3 rozporządzenia) oraz przekazują zatwierdzone plany do UKE (§ 10 ust. 1 rozporządzenia). W przypadku stwierdzenia braku kompletności planu, Prezes UKE ma obowiązek zwrócenia tego dokumentu przedsiębiorcy i wyznaczenia terminu jego uzupełnienia (§ 10 ust. 2 ww. rozporządzenia).

---

36 Przedmiotowe obowiązki UKE zostały wprowadzone do ustawy Prawo telekomunikacyjne z dniem 22 marca 2013 r. na podstawie ustawy z dnia 16 listopada 2012 r. o zmianie ustawy – Prawo telekomunikacyjne oraz niektórych innych ustaw (Dz. U. z 2012 r., poz. 1445 ze zm.).

37 Dz. U. Nr 15, poz. 77.

38 Uzgodnienia prowadzone są również z: Ministrem Obrony Narodowej, ministrem właściwym ds. wewnętrznych, ministrem właściwym ds. zagranicznych, ministrem właściwym ds. finansów publicznych, Ministrem Sprawiedliwości oraz Szefami ABW i AW.

Równolegle do opisanych powyżej regulacji dotyczących zadań przypisanych różnym instytucjom państwowym, powoływane były doraźne struktury organizacyjne, mające na celu reagowanie na zdarzenia i incydenty, które wystąpiły w cyberprzestrzeni. Podmiotami takimi były w szczególności:

- **Zespół zadaniowy do spraw ochrony portali rządowych**, powołany decyzją Przewodniczącego Komitetu Rady Ministrów do spraw Cyfryzacji Nr 1/2012 z dnia 24 stycznia 2012 r. w reakcji na ataki ACTA. Celami działania Zespołu było: wypracowanie wytycznych ochrony portali rządowych, ustalenie standardów bezpieczeństwa i polityki bezpieczeństwa dla stron rządowych, rekomendowanie Komitetowi Rady Ministrów do spraw Cyfryzacji decyzji strategicznych dla realizacji wytycznych i wdrożenia standardów bezpieczeństwa oraz jednolitej polityki bezpieczeństwa[39];
- Zespół do spraw incydentu bezpieczeństwa teleinformatycznego Kancelarii Prezesa Rady Ministrów, powołany na podstawie zarządzenia Nr 5 Szefa Kancelarii Prezesa Rady Ministrów z dnia 7 marca 2013 r. Do zadań Zespołu należało określenie przyczyn oraz ocena skutków nieuprawnionego dostępu do informacji przetwarzanych w systemie teleinformatycznym KPRM oraz przedstawienie propozycji działań korygujących i naprawczych.

Kluczowym aktem normatywnym określającym wymogi dla państwowych systemów i rejestrów informatycznych jest **ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne** (zwana dalej ustawą o informatyzacji). Zakres przedmiotowy ww. regulacji dotyczy przede wszystkim zapewnienia interoperacyjności (tj. współdziałania i wymiany danych) między różnymi systemami i bazami danych wykorzystywanymi przez podmioty państwowe do realizacji zadań publicznych. Zagadnienia dotyczące bezpieczeństwa danych przetwarzanych za pomocą systemów informatycznych zostały natomiast uwzględnione w wydanym na podstawie tej ustawy **rozporządzeniu 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**[40]. Zgodnie z § 20 ww. rozporządzenia, podmioty realizujące zadania publiczne zostały zobowiązane do wdrożenia i doskonalenia systemów zarządzania bezpieczeństwem informacji zapewniających poufność, dostępność, integralność i rozliczalność przetwarzanych informacji. W ramach zarządzania bezpieczeństwem informacji kierownicy ww. podmiotów zostali zobowiązani w szczególności do:

- przeprowadzania okresowych analiz ryzyka utraty integralności, dostępności i poufności informacji;
- zapewnienia, że osoby zaangażowane w proces przetwarzania informacji posiadają uprawnienia adekwatne do realizowanych przez nie zadań;
- zapewnienia szkolenia osób zaangażowanych w proces przetwarzania informacji;

[39] W skład Zespołu wchodzili przedstawiciele: ABW, MON, MSW, 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. Zespól został formalnie rozwiązany w dniu 13 czerwca 2014 r.

[40] Dz. U. z 2012 r., poz. 526 ze zm., zwane dalej rozporządzeniem w sprawie Krajowych Ram Interoperacyjności. Przedmiotowy akt prawny, w okresie objętym kontrolą, był poprzedzony rozporządzeniem Rady Ministrów z dnia 11 października 2005 r. w sprawie minimalnych wymagań dla systemów teleinformatycznych (Dz. U. Nr 212, poz. 1766).

- zapewnienia ochrony przetwarzanych informacji przed ich kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami;
- ustanowienia podstawowych zasad gwarantujących bezpieczną pracę przy przetwarzaniu mobilnym i pracy na odległość;
- zapewnienia odpowiedniego poziomu bezpieczeństwa systemów teleinformatycznych, polegającego w szczególności na: dbałości o aktualizację oprogramowania, minimalizowaniu ryzyka utraty informacji w wyniku awarii, stosowaniu mechanizmów kryptograficznych w sposób adekwatny do zagrożeń lub wymogów przepisu prawa, zapewnieniu bezpieczeństwa plików systemowych;
- bezzwłocznego zgłaszania incydentów naruszenia bezpieczeństwa informacji w określony i z góry ustalony sposób, umożliwiający szybkie podjęcie działań korygujących (w rozporządzeniu nie określono adresata zgłoszeń dotyczących incydentów, ani podmiotu zobowiązanego do podjęcia działań korygujących);
- zapewnienia okresowego (tj. nie rzadziej niż raz na rok) audytu wewnętrznego w zakresie bezpieczeństwa informacji.

Zgodnie z § 20 ust. 3 rozporządzenia w sprawie Krajowych Ram Interoperacyjności, system zarządzania bezpieczeństwem informacji przetwarzanych w systemach teleinformatycznych podmiotu publicznego spełnia wymogi tej regulacji, w przypadku gdy został opracowany na podstawie Polskiej Normy PN-ISO/IEC 27001[41] oraz jest wdrażany w oparciu o normy: PN-ISO/IEC 17799 (w odniesieniu do zabezpieczeń), PN-ISO/IEC 27005 (w odniesieniu do zarządzania ryzykiem) oraz PN-ISO/IEC 24762 (w odniesieniu do odtwarzania techniki informatycznej po katastrofie w ramach zarządzania ciągłością działania).

W art. 25 ustawy o informatyzacji wskazano podmioty uprawnione do przeprowadzania kontroli projektów i systemów teleinformatycznych dedykowanych do realizacji zadań publicznych oraz określono zakres przedmiotowy tych kontroli obejmujący m.in. badanie pod względem zgodności z minimalnymi wymaganiami dla systemów teleinformatycznych określonymi w rozporządzeniu w sprawie Krajowych Ram Interoperacyjności.

Zarządzanie kryzysowe

Ze względu na uzależnienie znacznej części państwowej infrastruktury krytycznej od technologii informatycznych i elektronicznego przekazywania danych, ochrona cyberprzestrzeni jest integralnie powiązana z procesem zarządzania kryzysowego.

Zgodnie z art. 2 **ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym**[42] termin zarządzanie kryzysowe obejmuje działalność organów administracji publicznej będącą elementem kierowania bezpieczeństwem narodowym, która polega na zapobieganiu sytuacjom kryzysowym, przygotowaniu do przejmowania nad nimi kontroli w drodze zaplanowanych działań, reagowaniu w przypadku wystąpienia sytuacji kryzysowych, usuwaniu ich skutków oraz odtwarzaniu zasobów i infrastruktury krytycznej. Pod pojęciem **sytuacji kryzysowej** należy rozumieć sytuację wpływającą negatywnie na poziom bezpieczeństwa ludzi, mienia w znacznych rozmiarach lub środowiska, wywołującą znaczne ograniczenia w działaniu właściwych organów administracji publicznej ze względu na nieadekwatność posiadanych sił i środków (art. 3 pkt 1 ww. ustawy). **Infrastrukturę krytyczną**

41 Określającej wymagania dotyczące budowania systemów zarządzania bezpieczeństwem informacji oraz kryteria ich oceny.

42 Dz. U. z 2013 r., poz. 1166.

państwa stanowią natomiast systemy oraz wchodzące w ich skład powiązane ze sobą funkcjonalnie obiekty, w tym obiekty budowlane, urządzenia, instalacje, usługi kluczowe dla bezpieczeństwa państwa i jego obywateli oraz służące zapewnieniu sprawnego funkcjonowania organów administracji publicznej, a także instytucji i przedsiębiorców. **Infrastruktura krytyczna obejmuje systemy**: zaopatrzenia w energię, surowce energetyczne i paliwa, łączności, sieci teleinformatycznych, finansowe, zaopatrzenia w żywność, zaopatrzenia w wodę, ochrony zdrowia, transportowe, ratownicze, zapewniające ciągłość działania administracji publicznej, produkcji, składowania, przechowywania i stosowania substancji chemicznych i promieniotwórczych, w tym rurociągi substancji niebezpiecznych (art. 3 pkt 2 ww. ustawy). Właściciele oraz posiadacze samoistni i zależni obiektów, instalacji lub urządzeń infrastruktury krytycznej (**operatorzy infrastruktury krytycznej**) mają obowiązek ich ochrony, w szczególności przez przygotowanie i wdrażanie, stosownie do przewidywanych zagrożeń, planów ochrony infrastruktury krytycznej oraz utrzymywanie własnych systemów rezerwowych zapewniających bezpieczeństwo i podtrzymujących funkcjonowanie tej infrastruktury, do czasu jej pełnego odtworzenia (art. 6 ust. 5 ww. ustawy).

Podstawą systemu zarządzania kryzysowego jest opracowywany przez Rządowe Centrum Bezpieczeństwa (RCB)[43] i przyjmowany w drodze uchwały przez Radę Ministrów – raport o zagrożeniach **bezpieczeństwa narodowego**[44]. Przedmiotowy dokument zawiera w szczególności mapę ryzyk dotyczących kluczowych zagrożeń dla funkcjonowania państwa i gospodarki oraz rekomendacje działań wymaganych w celu ich ograniczenia. Raport podlega aktualizacji nie rzadziej niż raz na dwa lata[45].

W oparciu m.in. o wnioski zwarte w ww. raporcie opracowywany jest **Narodowy Program Ochrony Infrastruktury Krytycznej** (zwany dalej NPOiK), określający m.in. narodowe priorytety, cele, wymagania i standardy, służące zapewnieniu sprawnego funkcjonowania infrastruktury krytycznej oraz ministrów kierujących działami administracji rządowej i kierowników urzędów centralnych odpowiedzialnych za poszczególne systemy infrastruktury krytycznej. Dyrektor RCB określa kryteria powalające na wyodrębnienie obiektów, instalacji, urządzeń i usług wchodzących w skład systemów infrastruktury krytycznej oraz na podstawie informacji przedkładanych przez ministrów i kierowników urzędów centralnych, opracowuje jednolity **wykaz infrastruktury krytycznej**. Następnie, w oparciu o szczegółowe informacje przekazywane przez ministrów i kierowników urzędów centralnych dotyczące będących w ich właściwości zasobów infrastruktury krytycznej, Dyrektor RCB opracowuje projekt NPOiK, który powinien zostać uzgodniony z jego uczestnikami, tj. zarówno z organami administracji publicznej i służbami odpowiedzialnymi za bezpieczeństwo narodowe, jak i operatorami infrastruktury krytycznej. Narodowy Program Ochrony Infrastruktury Krytycznej jest przyjmowany w drodze uchwały przez Radę Ministrów i podlega aktualizacji nie rzadziej niż raz na dwa lata[46]. Bezpośrednio po przyjęciu Programu, Dyrektor RCB informuje operatorów infrastruktury krytycznej o ujęciu podległych im zasobów i systemów w wykazie infrastruktury krytycznej[47].

---

43 Na podstawie raportów cząstkowych przedkładanych przez ministrów kierujących działami administracji rządowej, kierowników urzędów centralnych oraz wojewodów.

44 Raport o zagrożeniach bezpieczeństwa narodowego został przyjęty uchwałą Rady Ministrów z dnia 24 czerwca 2011 r. oraz znowelizowany na podstawie uchwały Rady Ministrów z dnia 12 lipca 2013 r.

45 Przedmiotowe zagadnienie reguluje art. 5a ustawy o zarządzaniu kryzysowym oraz rozporządzenie Rady Ministrów z dnia 30 kwietnia 2010 r. w sprawie Raportu o zagrożeniach bezpieczeństwa narodowego (Dz. U. Nr 83, poz. 540).

46 Narodowy Program Ochrony Infrastruktury Krytycznej został przyjęty uchwałą Radę Ministrów z dnia 26 marca 2013 r.

47 Przedmiotowe zagadnienie reguluje art. 5b ustawy o zarządzaniu kryzysowym oraz rozporządzenie Rady Ministrów z dnia 30 kwietnia 2010 r. w sprawie Narodowego Programu Ochrony Infrastruktury Krytycznej (Dz. U. Nr 83, poz. 541).

Operatorzy infrastruktury krytycznej są zobowiązani do opracowania, w terminie dziewięciu miesięcy od otrzymania od Dyrektora RCB informacji o ujęciu w ww. wykazie, **planów ochrony infrastruktury krytycznej**, a następnie uzgodnienia ich treści z właściwymi organami[48]. Przedmiotowe plany zawierają m.in.: informacje na temat danego obiektu infrastruktury krytycznej, charakterystykę zagrożeń oraz ocenę ryzyka ich wystąpienia, warianty działania w sytuacji zagrożenia lub zakłócenia funkcjonowania infrastruktury, warianty zapewnienia ciągłości funkcjonowania oraz odtwarzania infrastruktury krytycznej. Plany ochrony infrastruktury krytycznej są przekazywane do Dyrektora RCB, który dokonuje zatwierdzenia tych dokumentów[49].

W oparciu o wnioski wynikające z raportu o zagrożeniach bezpieczeństwa narodowego, w RCB opracowywany jest również we współpracy z ministerstwami i urzędami centralnymi **Krajowy Plan Zarządzania Kryzysowego**[50], obejmujący w szczególności:

- charakterystykę zagrożeń, ocenę ryzyka ich wystąpienia i zadania w zakresie monitorowania zagrożeń;
- zadania i obowiązki uczestników zarządzania kryzysowego;
- zestawienie sił i środków planowanych do wykorzystania w sytuacjach kryzysowych;
- tryb uruchamiania niezbędnych sił i środków uczestniczących w realizacji planowanych przedsięwzięć na wypadek sytuacji kryzysowej;
- procedury reagowania kryzysowego, określające sposób postępowania w sytuacjach kryzysowych[51].

Podmiotem odpowiedzialnym za zarządzanie kryzysowe na terytorium Rzeczpospolitej Polskiej jest Rada Ministrów. W przypadkach niecierpiących zwłoki zarządzanie kryzysowe sprawuje minister właściwy do spraw wewnętrznych, zawiadamiając niezwłocznie o swoich działaniach Prezesa Rady Ministrów (art. 7 ust. 1 i 2 ustawy o zarządzaniu kryzysowym). Obsługę Rady Ministrów, Prezesa Rady Ministrów i ministra właściwego do spraw wewnętrznych w sprawach zarządzania kryzysowego pełni RCB, do którego zadań (oprócz wymienionych powyżej) należy m.in.: gromadzenie informacji o zagrożeniach oraz analiza i ocena możliwości wystąpienia zagrożeń lub ich rozwoju, wypracowywanie propozycji zapobiegania zagrożeniom (art. 11 ust. 1 i 2 ww. ustawy). Organy właściwe w sprawach zarządzania kryzysowego oraz Dyrektor RCB mają prawo żądania udzielenia informacji, gromadzenia i przetwarzania danych niezbędnych do realizacji zadań określonych w ustawie (art. 20a powołanej ustawy).

Międzynarodowe regulacje prawne dotyczące przestępczości i zagrożeń w cyberprzestrzeni

Istniejące międzynarodowe regulacje prawne w zakresie szeroko rozumianych incydentów występujących w cyberprzestrzeni dotyczą przede wszystkim harmonizacji prawa karnego oraz ustanowienia mechanizmów współpracy między właściwymi organami różnych państw odpowiadającymi za zwalczanie przestępczości, w celu umożliwienia ścigania przestępstw

48 M.in. z ministrem lub kierownikiem urzędu centralnego, we właściwości którego znajduje się system, do którego została zaliczona dana infrastruktura krytyczna.

49 Przedmiotowe zagadnienie reguluje art. 6 ust. 5 ustawy o zarządzaniu kryzysowym oraz rozporządzenie Rady Ministrów z dnia 30 kwietnia 2010 r. w sprawie planów ochrony infrastruktury krytycznej (Dz. U. Nr 83, poz. 542).

50 Plany zarządzania kryzysowego są również tworzone w ministerstwach i w urzędach centralnych oraz w poszczególnych województwach, powiatach i gminach.

51 Art. 5, art. 11 ust. 2 pkt 1 lit. b oraz art. 12 ust. 2 i 2a ustawy o zarządzaniu kryzysowym. Krajowy Plan Zarządzania Kryzysowego został przyjęty uchwałą Rady Ministrów z dnia 6 marca 2012 r. oraz znowelizowany na podstawie uchwały Rady Ministrów z dnia 23 lipca 2013 r.

popełnianych z wykorzystaniem systemów informatycznych oraz w stosunku do przechowywanych w nich danych. Przykładami takich regulacji są:

- Dyrektywa Parlamentu Europejskiego i Rady 2013/40/UE z dnia 12 sierpnia 2013 r. dotycząca ataków na systemy informatyczne i zastępująca decyzję ramową Rady 2005/222/WSiSW[52];
- Konwencja Rady Europy o cyberprzestępczości z dnia 23 listopada 2001 r.[53] (tzw. Konwencja budapesztańska).

Bezpieczeństwo cyberprzestrzeni rozumiane jako zapobieganie i minimalizacja skutków incydentów jest natomiast jednym z istotnych obszarów zainteresowania Unii Europejskiej, o czym świadczy m.in. powołanie w 2004 r. wyspecjalizowanej Europejskiej Agencji do spraw Bezpieczeństwa Sieci i Informacji.

W dniu 7 lutego 2013 r. Komisja Europejska przedstawiła wspólny komunikat do Parlamentu Europejskiego, Rady Unii Europejskiej oraz Komitetu Ekonomiczno-Społecznego i Komitetu Regionów dotyczący Strategii bezpieczeństwa cybernetycznego Unii Europejskiej[54] razem z **wnioskiem legislacyjnym dotyczącym Dyrektywy Parlamentu Europejskiego i Rady w sprawie środków mających na celu zapewnienie wspólnego wysokiego poziomu bezpieczeństwa sieci i informacji w obrębie Unii** (zwanej dalej dyrektywą NIS)[55]. W projekcie dyrektywy zawarto precyzyjne i daleko idące zobowiązania państw członkowskich dotyczące w szczególności:

1. Przyjęcia **krajowej strategii w zakresie bezpieczeństwa sieci i informacji** określającej cele strategiczne oraz konkretne środki polityczne i regulacyjne mające na celu osiągnięcie wysokiego poziomu bezpieczeństwa sieci i informacji. Krajowa strategia powinna obejmować **krajowy plan współpracy w zakresie bezpieczeństwa sieci i informacji**[56], zawierający co najmniej[57]:
   - plan oceny zagrożeń umożliwiający określenie zagrożeń i ocenę wpływu potencjalnych incydentów;
   - określenie funkcji i obowiązków poszczególnych podmiotów zaangażowanych w realizację planu;
   - procedury współpracy i komunikacji zapewniające zapobieganie, wykrywanie, reagowanie, naprawę i przywrócenie stanu normalnego, dostosowane do poziomu stanu alarmowego;
   - plan ćwiczeń i szkoleń[58] w zakresie bezpieczeństwa sieci i informacji, mający na celu ulepszenie, zatwierdzenie i sprawdzenie planu współpracy.

52 Dz.U. L 218 z 12.08.2013 r. s.8. Przedmiotowa dyrektywa była poprzedzona Decyzją Ramową Rady 2005/222/WSiSW z dnia 24 lutego 2005 r. w sprawie ataków na systemy informatyczne (Dz.U. L 69 z 24.02.2005 r., s.67).

53 Konwencja weszła w życie 1 lipca 2004 r., natomiast dopiero w listopadzie 2014 r. została ratyfikowana przez Polskę.

54 JOIN(2013) 1 final.

55 COM(2013) 48 final.

56 Zgodnie z art. 5 ust 3 projektu dyrektywy, krajowa strategia w zakresie bezpieczeństwa sieci i informacji oraz krajowy plan współpracy w zakresie bezpieczeństwa sieci i informacji powinny być przekazywane do Komisji w ciągu jednego miesiąca od ich przyjęcia.

57 Art. 5. projektu dyrektywy.

58 Wnioski wypływające z przeprowadzanych ćwiczeń powinny być dokumentowane i na bieżąco włączane do zaktualizowanych wersji planu.

2. Wyznaczenia **właściwego krajowego organu ds. bezpieczeństwa sieci i systemów informatycznych**. Państwa członkowskie powinny zapewnić właściwym organom odpowiednie zasoby techniczne, finansowe i ludzkie oraz wyposażyć je w uprawnienia do[59]:
   - otrzymywania od organów administracji publicznej i podmiotów gospodarczych[60] zgłoszeń dotyczących incydentów;
   - badania przypadków niewypełniania przez organy administracji publicznej i podmioty gospodarcze ciążących na nich zobowiązań w zakresie zabezpieczenia systemów i sieci oraz informowania o incydentach;
   - żądania od podmiotów gospodarczych i organów administracji publicznej przekazywania informacji potrzebnych do oceny bezpieczeństwa ich sieci i systemów informatycznych oraz poddawania się audytowi bezpieczeństwa;
   - wydawania wiążących instrukcji dla podmiotów gospodarczych i organów administracji publicznej.
3. Ustanowienia **zespołu CERT** odpowiadającego m.in. za: monitorowanie incydentów na poziomie krajowym, przekazywanie ostrzeżeń, ogłaszanie alarmów, reagowanie na incydenty oraz prowadzenie współpracy z sektorem prywatnym. Zespół CERT powinien zapewniać wysoką dostępność swoich usług oraz działać według jasno określonej procedury. Obowiązkiem państw członkowskich jest zapewnienie zespołowi CERT odpowiednich zasobów technicznych, finansowych i ludzkich oraz bezpiecznej infrastruktury komunikacyjnej. CERT powinien działać pod nadzorem właściwego krajowego organu ds. bezpieczeństwa sieci i systemów informatycznych, który regularnie dokonuje przeglądu stosowności jego zasobów, mandatu oraz skuteczności postępowania w przypadku incydentów[61].
4. Zapewnienia zastosowania przez organy administracji publicznej i podmioty gospodarcze właściwych środków technicznych i organizacyjnych w celu przeciwdziałania zagrożeniom, na jakie narażone są kontrolowane i wykorzystywane przez nie sieci i systemy informatyczne oraz zobowiązanie tych podmiotów do zgłaszania informacji o incydentach[62].

W art. 8 – 11 projektu dyrektywy określono również założenia aktywnego **systemu współpracy i wymiany informacji państw członkowskich** w zakresie przeciwdziałania i reagowania na zagrożenia i incydenty dotyczące sieci i systemów informatycznych.

Wg stanu na dzień podpisania niniejszej informacji, projekt dyrektywy NIS został przyjęty z poprawkami przez Parlament Europejski (13 marca 2014 r.) i oczekuje na pierwsze czytanie w Radzie Unii Europejskiej. W toku dotychczasowych prac w Parlamencie Europejskim i w organach Rady, zostały zgłoszone poprawki w sposób istotny ograniczające oddziaływanie planowanej dyrektywy, zarówno w zakresie obowiązków poszczególnych państw członkowskich, jak i w odniesieniu do mechanizmów współpracy w ramach UE. Planowane jest także wydłużenie okresu implementacji przepisów dyrektywy z 18 do 30 miesięcy.

59 Art. 6, 14 ust. 2 oraz art. 15 ust. 1–3 projektu dyrektywy.

60 Tj. dostawcy usług społeczeństwa informacyjnego oraz operatorzy infrastruktury krytycznej.

61 Art. 7 oraz załącznik nr 1 do projektu dyrektywy.

62 Art. 14 projektu dyrektywy.

3.2 Istotne ustalenia kontroli

3.2.1. Budowa systemu ochrony cyberprzestrzeni RP

Opracowanie narodowej strategii ochrony cyberprzestrzeni

NIK ocenia negatywnie fakt, że Rada Ministrów i kierownictwo podmiotów administracji państwowej nie opracowały dotychczas narodowej strategii ochrony cyberprzestrzeni Polski, która mogłaby być podstawą konkretnych, systemowych działań podnoszących poziom bezpieczeństwa teleinformatycznego państwa. W ocenie NIK, prowadzone w latach 2008–2014, działania mające na celu przygotowanie i uzgodnienie strategicznego dokumentu dotyczącego bezpieczeństwa teleinformatycznego państwa były realizowane w sposób nierzetelny i bez należytego przygotowania.

Od 2008 r., w ówczesnym Ministerstwie Spraw Wewnętrznych i Administracji (MSWiA) oraz m.in. w ABW prowadzone były czynności mające na celu przygotowanie kompleksowej, narodowej strategii przeciwdziałania zagrożeniom występującym w cyberprzestrzeni. W toku ww. prac powstało siedem kolejnych projektów strategii:

- „Rządowy program ochrony cyberprzestrzeni RP na lata 2008–2011" (listopad 2008 r.);
- „Rządowy program ochrony cyberprzestrzeni RP na lata 2009–2011" (styczeń 2009 r.);
- „Rządowy program ochrony cyberprzestrzeni RP na lata 2009–2011" – założenia (marzec 2009 r);
- „Rządowy program ochrony cyberprzestrzeni RP na lata 2011–2015" (maj 2010 r.);
- „Rządowy program ochrony cyberprzestrzeni RP na lata 2011–2016" (czerwiec 2010 r.);
- „Rządowy program ochrony cyberprzestrzeni RP na lata 2011–2020" (kwiecień 2011 r.);
- „Polityka bezpieczeństwa cyberprzestrzeni RP" (maj 2011 r.).

Żaden z wymienionych dokumentów nie został zatwierdzony przez Radę Ministrów i przyjęty do realizacji, co wynikało przede wszystkim z ich niskiej jakości oraz nierzetelnego przygotowania. We wszystkich projektach nie zawarto precyzyjnie określonych celów, mierników oraz terminów realizacji zadań, a także podmiotów odpowiedzialnych za ich wykonanie. Nie oszacowano kosztów planowanych działań, ani nie wskazano źródeł ich finansowania. Nie opracowano także konkretnych projektów zmian legislacyjnych niezbędnych do wprowadzenia w celu budowy krajowego systemu ochrony cyberprzestrzeni.

Drugim czynnikiem, który uniemożliwił efektywne prace nad narodową strategią ochrony cyberprzestrzeni były sprzeczne interesy i stanowiska kierownictwa poszczególnych podmiotów uczestniczących w uzgodnieniach międzyresortowych kolejnych projektów tego dokumentu. Przedmiotem sporu były w szczególności:

- postulaty Ministra Rozwoju Regionalnego dotyczące doprecyzowania zapisów strategii, poprzez podanie szczegółowych mierników, terminów, kosztów oraz źródeł finansowania poszczególnych zadań;
- zdecydowane stanowisko Ministra Finansów oraz przedstawicieli Kancelarii Prezesa Rady Ministrów wskazujące na brak możliwości przeznaczenia jakichkolwiek dodatkowych środków finansowych na realizację działań związanych z bezpieczeństwem teleinformatycznym oraz postulat wykreślenia kwestii finansowania zadań ze strategii;

- wątpliwości prawne dotyczące pożądanej formy dokumentu określającego narodową strategię ochrony cyberprzestrzeni (np. program, polityka itd.) oraz możliwości nakładania przez taki dokument konkretnych obowiązków na podmioty spoza administracji rządowej;
- rozbieżne stanowiska oraz współzawodnictwo kierownictwa MSWiA i ABW w zakresie pożądanej struktury koordynacji systemu ochrony cyberprzestrzeni, w tym spory personalne dotyczące powołania i obsadzenia stanowiska Pełnomocnika Rządu ds. Ochrony Cyberprzestrzeni RP.

W rezultacie, prowadzone przez kilka lat, międzyresortowe uzgodnienia narodowej strategii ochrony cyberprzestrzeni, zamiast poszukiwania optymalnych merytorycznie rozwiązań podnoszących bezpieczeństwo teleinformatyczne państwa, koncentrowały się na wypracowaniu źle rozumianego kompromisu między różnymi instytucjami publicznymi. Polegały one na usuwaniu wszystkich spornych fragmentów tego dokumentu oraz takim przeredagowaniu jego treści, aby ogólne sformułowania nie wzbudzały kontrowersji wśród jego recenzentów i potencjalnych wykonawców. **W ocenie NIK, opisane uzgodnienia stanowią modelowy przykład zjawiska nazywanego potocznie „Polską resortową", którego istotą jest postrzeganie zadań publicznych wyłącznie przez pryzmat obowiązków i interesów poszczególnych urzędów (bez dostrzegania ich szerszego kontekstu) oraz niezdolność do współdziałania różnych instytucji państwowych**. Brak rzetelnej i efektywnej współpracy kluczowych podmiotów odpowiadających za bezpieczeństwo teleinformatyczne, skutkował kilkuletnim opóźnieniem w przyjęciu narodowej strategii ochrony cyberprzestrzeni oraz istotnym i konsekwentnym spadkiem jakości kolejnych projektów rządowych dokumentów opracowanych w tym zakresie. O ile bowiem pierwsze projekty (w tym w szczególności „Rządowy program ochrony cyberprzestrzeni RP na lata 2011-2016"), stanowiły przynajmniej próbę kompleksowego podejścia do kwestii ochrony cyberprzestrzeni, to kolejne dokumenty przygotowywane w tym zakresie były już tylko próbą wypracowania zapisów akceptowalnych dla poszczególnych instytucji.

W styczniu 2012 r., w reakcji na wydarzenia związane z protestami ACTA, w nowo utworzonym MAiC, wznowiono prace prowadzone wcześniej w byłym MSWiA, mające na celu przygotowanie narodowej strategii ochrony cyberprzestrzeni. W wyniku ww. prac, przygotowano projekt dokumentu pt. „**Polityka Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej**", 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. **„Polityka" została przyjęta uchwałą Rady Ministrów Nr 111/2013 z dnia 25 czerwca 2013 r.**, a koordynację realizacji jej postanowień powierzono ministrowi właściwemu ds. informatyzacji. W pkt 1.4. „Polityki" wskazano, że jest ona dokumentem obowiązującym administrację rządową oraz jest rekomendowana dla administracji samorządowej i innych państwowych osób prawnych i jednostek organizacyjnych. W przypadku pozostałych użytkowników cyberprzestrzeni (np. przedsiębiorców, prywatnych operatorów infrastruktury krytycznej) „Polityka" ma stanowić wskazówkę do prowadzonych przez nich działań.

Przeprowadzona kontrola wykazała, że działania Ministra Administracji i Cyfryzacji mające na celu opracowanie narodowej strategii ochrony cyberprzestrzeni były realizowane 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 oraz nie wykorzystywano dostępnych w tym zakresie wzorów dobrych praktyk[63], i tak:

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

- przygotowanie projektu „Polityki" nie zostało poprzedzone opracowaniem katalogu kluczowych dla funkcjonowania państwa systemów teleinformatycznych, które powinny podlegać ochronie. Minister Administracji i Cyfryzacji nie posiadał podstawowej wiedzy na temat najważniejszych wykorzystywanych w Polsce (przez podmioty państwowe i prywatne) systemów teleinformatycznych oraz nie współpracował z RCB, w celu określenia kryteriów identyfikacji takich systemów oraz ewentualnego wykorzystania opracowanego przez ten podmiot wykazu infrastruktury krytycznej (w zakresie ujętych w tym wykazie systemów teleinformatycznych). Nie dysponował również wiedzą na temat systemów teleinformatycznych wykorzystywanych do realizacji zadań publicznych. Prowadzono więc prace nad narodową strategią ochrony cyberprzestrzeni bez uprzedniego uzyskania odpowiedzi na fundamentalne pytanie, wynikające m.in. z uznanych międzynarodowych wzorów dobrych praktyk, tj. jakie zasoby i w jakim zakresie należy w pierwszej kolejności chronić, żeby uniknąć zakłóceń w funkcjonowaniu państwa spowodowanych atakiem cybernetycznym;
- 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 bezpieczeństwem teleinformatycznym i przyjęciem narodowej strategii ochrony cyberprzestrzeni. Skutkowało to brakiem ciągłości realizacji zadań państwa w tym zakresie i potrzebą rozpoczęcia wszystkich prac, po upływie kilku lat, całkowicie od nowa;
- nie została przeprowadzona kompleksowa inwentaryzacja obowiązujących aktów prawnych związanych z ochroną cyberprzestrzeni oraz nie podjęto żadnych prób oszacowania zasobów i kosztów niezbędnych do realizacji działań wskazanych w „Polityce".

Brak przeprowadzenia podstawowych analiz niezbędnych do rzetelnego opracowania narodowej strategii ochrony cyberprzestrzeni, wynikał w szczególności z faktu, że MAiC było całkowicie nieprzygotowane kadrowo i organizacyjnie do realizacji tych zadań (kwestia zasobów Ministerstwa została szczegółowo opisana na str. 41 niniejszej informacji). W związku z powyższym, główny ciężar prac nad strategią ochrony cyberprzestrzeni oraz kluczowe decyzje dotyczące jej treści zostały nieformalnie przejęte[64] przez funkcjonujący przy Komitecie Rady Ministrów ds. Cyfryzacji – „Zespół zadaniowy do spraw ochrony portali rządowych".

W ocenie NIK, przygotowanie „Polityki" przez Zespół zadaniowy wpłynęło negatywnie na jakość tego dokumentu. Wynikało to z faktu, iż został on powołany w reakcji na konkretne wydarzenia związane z atakami na strony rządowe w trakcie protestów ACTA i jego zadania ograniczały się do ochrony portali oraz stron internetowych instytucji publicznych. Zadania ww. Zespołu zdeterminowały zatem w znacznym stopniu treść i zakres podmiotowy „Polityki" oraz wpłynęły na ograniczenie jej obowiązywania do podmiotów administracji rządowej. Ponadto, uwzględniając wieloletnie, bezskuteczne działania w celu przyjęcia narodowej strategii bezpieczeństwa cyberprzestrzeni, członkowie Zespołu zrezygnowali z wypracowania kompleksowej, systemowej strategii i skoncentrowali się na pośpiesznym przygotowaniu kompromisowego, ogólnego dokumentu będącego reakcją ad hoc na wydarzenia ACTA. Świadczy o tym m.in. fakt konsekwentnego usuwania z kolejnych projektów „Polityki" wszystkich spornych fragmentów

[64] Zgodnie z art. 7 ust. 2 ustawy z dnia 8 sierpnia 1996 r. o Radzie Ministrów (Dz. U. z 2012 r., poz. 392 ze zm.) oraz § 20 uchwały Nr 190 Rady Ministrów z dnia 29 października 2013 r. Regulamin pracy Rady Ministrów (M.P. z 2013 r., poz. 979.), Minister Administracji i Cyfryzacji był organem uprawnionym do opracowania, prowadzenia uzgodnień i wniesienia projektu „Polityki" do rozpatrzenia przez Radę Ministrów. Na wszystkich etapach prac nad ww. dokumentem organem wnioskującym i prowadzącym proces jego uzgodnień był Minister Administracji i Cyfryzacji.

wprowadzających jakiekolwiek precyzyjne zobowiązania podmiotów państwowych, dotyczących m.in. sporządzenia i przekazania Prezesowi Rady Ministrów zbiorczego sprawozdania z szacowania ryzyka związanego z funkcjonowaniem cyberprzestrzeni oraz propozycji zmian legislacyjnych.

Nierzetelne przygotowanie, w ocenie NIK, spowodowało niską jakość oraz liczne błędy merytoryczne „Polityki" dotyczące w szczególności:

- **nieprecyzyjnego i ogólnego charakteru dokumentu** – w „Polityce" nie określono: celów, produktów, mierników, terminów realizacji poszczególnych zadań, ani (poza pojedynczymi przypadkami) podmiotów odpowiedzialnych za ich wykonanie. Nie wskazano również żadnych propozycji zmian legislacyjnych koniecznych do wprowadzenia w celu budowy systemu ochrony cyberprzestrzeni RP, ani projektów szczegółowych, które zgodnie z zapisami „Polityki", miały służyć wdrażaniu tego dokumentu w poszczególnych obszarach związanych z poprawą bezpieczeństwa teleinformatycznego. Zapisy „Polityki", w wielu punktach, zostały sformułowane w sposób nienormatywny i niejednoznaczny (z użyciem trybu przypuszczającego), w związku z czym nie określały one jednoznacznie i precyzyjnie zobowiązań podmiotów państwowych. **Kierownictwo objętych kontrolą podmiotów, w tym, co należy podkreślić – Minister Administracji i Cyfryzacji odpowiadający za koordynację wdrażania „Polityki" wyjaśniali, że nie rozumieją poszczególnych zapisów tego dokumentu i nie wiedzą, jakie zadania na jego podstawie powinni realizować**. Zgłaszane kontrolującym wątpliwości interpretacyjne odnosiły się do najważniejszych punktów tego dokumentu, dotyczących m.in. krajowego systemu reagowania na incydenty komputerowe oraz projektów szczegółowych;
- **nieprawidłowego zakresu podmiotowego dokumentu** – bezpośredni zakres obowiązywania „Polityki" został ograniczony do podmiotów administracji rządowej (bez adekwatnego odniesienia do podmiotów prywatnych, administracji samorządowej oraz innych użytkowników i administratorów cyberprzestrzeni), co stanowiło całkowite odstąpienie od założeń przyjętych na początku prac nad narodową strategią ochrony cyberprzestrzeni, wskazujących na priorytetowe znaczenie wdrożenia efektywnych mechanizmów ochrony krytycznej infrastruktury teleinformatycznej oraz współpracy w tym zakresie między podmiotami prywatnymi i państwowymi. Kierownictwo MAiC wyjaśniło, że zakres podmiotowy „Polityki" wynikał z faktu, że nie mogła ona nakładać obowiązków na podmioty spoza administracji rządowej, a ponadto zagadnienia dotyczące ochrony infrastruktury krytycznej zostały już uregulowane w ustawie o zarządzaniu kryzysowym.

  W ocenie NIK, nie ulega wątpliwości, że zasobami IT, kluczowymi z punktu widzenia ciągłości działania państwa, są (publiczne i prywatne) systemy oraz sieci teleinformatyczne wchodzące w skład infrastruktury krytycznej. Skuteczny atak cybernetyczny wymierzony w teleinformatyczną infrastrukturę krytyczną (np. systemy: energetyczny, finansowy, ochrony zdrowia, itp.) mógłby powodować trudne do oszacowania straty gospodarcze i społeczne, w tym bezpośrednie zagrożenie dla życia i zdrowia wielu osób (szacunkowa skala incydentów z ostatnich lat została wskazana na str. 57–58 niniejszej informacji). Całkowite pominięcie tego obszaru i ograniczenie narodowej strategii ochrony cyberprzestrzeni do zasobów IT administracji rządowej (z których istotna część nie ma w rzeczywistości krytycznego znaczenia, a tylko „wizerunkowe" – tak jak w przypadku stron rządowych zaatakowanych w trakcie protestów ACTA), **świadczy o błędnym i fragmentarycznym postrzeganiu kwestii bezpieczeństwa teleinformatycznego**

państwa[65]. Nie jest również uprawnione stwierdzenie, że zakres podmiotowy „Polityki" wynikał z ograniczeń prawnych. „Polityka" została przyjęta uchwałą Rady Ministrów, która jest aktem prawa wewnętrznego obowiązującym podmioty administracji rządowej, natomiast w treści tego dokumentu mogły być wskazane konkretne, proponowane przez rząd zmiany legislacyjne, związane z ochroną cyberprzestrzeni, regulujące obowiązki innych (państwowych i prywatnych) podmiotów np. z zakresu zarządzania kryzysowego. Ponadto, jak wskazano już wcześniej, ograniczony zakres podmiotowy „Polityki" wynikał w znacznym stopniu z przesłanek „pozamerytorycznych", tj. z dążenia do szybkiego i kompromisowego wypracowania jakiegokolwiek dokumentu, będącego reakcją na wydarzenia ACTA;

- **niewskazania kosztów i źródeł finansowania zadań związanych z ochroną cyberprzestrzeni** – w związku ze stanowiskiem Ministra Finansów wskazującym na konieczność „bezkosztowego" prowadzenia działań w obszarze bezpieczeństwa teleinformatycznego, w pkt 5. „Polityki" wskazano, że jej wdrażanie, w pierwszym roku obowiązywania, nie będzie implikować dodatkowych wydatków oraz ustanowiono nieprecyzyjny mechanizm szacowania tych kosztów w latach kolejnych (tematyka zasobów przypisanych do ochrony cyberprzestrzeni została szczegółowo opisana na str. 40–44 niniejszej informacji).

Stwierdzone przez NIK błędy merytoryczne „Polityki" były m.in. przedmiotem licznych uwag instytucji pozarządowych[66] zgłoszonych na etapie konsultacji społecznych projektu tego dokumentu. Przedmiotowe uwagi nie zostały jednak właściwie wykorzystane przez Ministra Administracji i Cyfryzacji. **W rezultacie, w ocenie NIK, „Polityka" jest opracowaniem wadliwym, pozbawionym podstawowych cech dokumentu strategicznego i ma jedynie charakter propagandowy** – manifestujący zaangażowanie rządu polskiego w ochronę cyberprzestrzeni. Nie istnieje natomiast możliwość wykorzystania „Polityki" w celu rzeczywistej poprawy bezpieczeństwa teleinformatycznego państwa. Przedstawioną ocenę potwierdzają ustalenia niniejszej kontroli wskazujące, że dwa lata od wejścia w życie, „Polityka" jest dokumentem martwym i nierealizowanym w praktyce. Stwierdzono także, że Minister Administracji i Cyfryzacji odpowiadający za wdrażanie „Polityki", nie podejmował działań wymienionych w pkt 1.5. oraz 6. tego dokumentu, dotyczących przeglądów treści, aktualizacji i poprawiania jego jakości. **W opinii Ministra „Polityka" powinna być dokumentem nieprecyzyjnym, wyznaczającym tylko „ogólne kierunki działań", a faktyczna budowa krajowego systemu ochrony cyberprzestrzeni, może zostać rozpoczęta dopiero po przyjęciu dyrektywy UE regulującej te zagadnienia**.

Niezależnie od prac koordynowanych przez Ministra Administracji i Cyfryzacji[67], czynności mające na celu stworzenie dokumentu strategicznego, dotyczącego bezpieczeństwa teleinformatycznego państwa były prowadzone również przez Biuro Bezpieczeństwa Narodowego. Efektem tych prac było przyjęcie w styczniu 2015 r. „Doktryny Cyberbezpieczeństwa Rzeczypospolitej Polskiej". W ocenie NIK, „Doktryna" stanowi wkład w zwiększanie świadomości zagrożeń występujących w cyberprzestrzeni, natomiast tak samo jak „Polityka" jest dokumentem ogólnym, niewskazującym jasno określonych zadań, podmiotów odpowiedzialnych za ich realizację oraz kosztów i źródeł finansowania.

---

65 Analogiczne stanowisko zostało przedstawione w opracowanej dla NIK ekspertyzie zewnętrznej - Instytut Kościuszki, „Propozycja modelowych rozwiązań w zakresie budowania cyberbezpieczeństwa Polski", Kraków 2015.

66 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.

67 Poprzednio, w okresie objętym kontrolą – Ministra Spraw Wewnętrznych i Administracji.

W ocenie NIK, należy podkreślić, że po upływie 7 lat od rozpoczęcia prac, w Polsce nie stworzono dokumentu stanowiącego podstawę realnych działań w zakresie zarządzania i reagowania na zdarzenia występujące w cyberprzestrzeni. Konieczne jest zatem podjęcie pilnych, wiążących decyzji dotyczących kształtu systemu ochrony cyberprzestrzeni w Polsce.

Identyfikacja zadań związanych z ochroną cyberprzestrzeni

Kontrola wykazała, że kierownictwo najważniejszych instytucji publicznych nie posiada świadomości zagrożeń związanych z funkcjonowaniem cyberprzestrzeni oraz wynikających z tego faktu nowych zadań administracji państwowej. Pomimo tego, że coraz większa część usług publicznych oraz istotnych aspektów życia społecznego i gospodarczego odbywa się obecnie w sieci Internet lub realizowana jest z wykorzystaniem systemów teleinformatycznych, bezpieczeństwo państwa w dalszym ciągu jest postrzegane jedynie z punktu widzenia zagrożeń konwencjonalnych, wymagających ochrony fizycznej, bez uwzględnienia postępujących zmian technologicznych i wzrostu zagrożeń w cyberprzestrzeni.

Ustalono w szczególności, że Minister Administracji i Cyfryzacji, który w chwili obecnej jest jedynym organem, któremu wprost przypisano zadania związane z ochroną cyberprzestrzeni, nie posiadał podstawowej świadomości obowiązków w tym zakresie. Minister nie zgodził się, iż odpowiada za koordynację działań pozostałych podmiotów państwowych związanych z bezpieczeństwem teleinformatycznym oraz wskazał, że w jego ocenie, zadania te nie wynikają z kierowania działami administracji rządowej „informatyzacja" i „łączność", ani z uchwały Rady Ministrów w sprawie przyjęcia „Polityki". W ocenie Kierownictwa MAiC, również przepisy dotyczące: zarządzania kryzysowego, ochrony infrastruktury krytycznej, informatyzacji, interoperacyjności, czy elektronicznego świadczenia usług nie łączą się bezpośrednio z tematyką ochrony cyberprzestrzeni i nie nakładają na Ministra Administracji i Cyfryzacji żadnych zadań w tym obszarze. W opinii Ministra, działalność MAiC w zakresie bezpieczeństwa teleinformatycznego ma charakter „dobrowolny" i powinna zasadniczo ograniczać się tylko do zasobów IT administracji rządowej. Powyższe stanowisko, przedstawione w związku z kontrolą NIK, znajdowało również wyraz w oficjalnej działalności oraz korespondencji MAiC. Przykładowo, we wrześniu 2012 r., w ramach realizacji obowiązku wynikającego z ustawy o zarządzaniu kryzysowym, MAiC przekazało do RCB i ABW raport cząstkowy o zagrożeniach bezpieczeństwa narodowego, obejmujący działy administracji rządowej kierowane przez Ministra Administracji i Cyfryzacji. W raporcie, zagrożenia występujące w cyberprzestrzeni RP zostały ograniczone do cyberterroryzmu, 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. (…)". Raport cząstkowy Ministra Administracji i Cyfryzacji o zagrożeniach bezpieczeństwa narodowego nie został skorygowany, pomimo otrzymania od ABW uwag wskazujących na braki merytoryczne w przyjętej przez MAiC definicji zagrożeń występujących w cyberprzestrzeni oraz na konieczność jego dostosowania do zapisów opracowanego w MAiC projektu „Polityki".

Brak świadomości zagrożeń związanych z funkcjonowaniem cyberprzestrzeni oraz wynikających z tego faktu obowiązków administracji państwowej, stwierdzono także w wyniku kontroli przeprowadzonej w MSW. **Ustalono, że od momentu wyodrębnienia tego Ministerstwa z MSWiA, w listopadzie 2011 r., Minister Spraw Wewnętrznych odpowiadający za sprawy bezpieczeństwa i zarządzania kryzysowego nie realizował żadnych zadań związanych z bezpieczeństwem państwa i jego infrastruktury w kontekście ochrony teleinformatycznej**. W szczególności, Minister nie podejmował działań w celu zawarcia w Krajowym Planie Zarządzania Kryzysowego procedur reagowania na zdarzenia związane z cyberprzestrzenią, co wyjaśniano niezidentyfikowaniem przez właściwe komórki Ministerstwa ryzyk w tym obszarze. MSW nie współpracowało również efektywnie z przedsiębiorcami telekomunikacyjnymi w realizacji nałożonych na nich obowiązków, dotyczących przygotowania planów działań w sytuacjach szczególnych zagrożeń. Minister Spraw Wewnętrznych, przekazując przedsiębiorcom informacje służące identyfikacji ryzyk dla ich działalności[68], nie wskazywał żadnych zagrożeń związanych z cyberprzestrzenią i rutynowo przedstawiał coroczną „Ocenę zagrożenia bezpieczeństwa powszechnego w Polsce", odnoszącą się wyłącznie do zagrożeń konwencjonalnych, takich jak powodzie, trzęsienia ziemi, pożary itd. Minister wyjaśnił, że nie informowano o ryzykach związanych z bezpieczeństwem teleinformatycznym, ponieważ obowiązujące przepisy nie nakładają wprost obowiązku przekazywania przedsiębiorcom informacji na temat tej konkretnej kategorii zagrożeń. Działania Ministra Spraw Wewnętrznych w obszarze bezpieczeństwa IT ograniczały się do własnych sieci oraz systemów resortowych, natomiast były one prowadzone bez należytego przygotowania oraz bez wdrożenia w MSW zapisów „Polityki".

W ocenie NIK, zagrożenia związane ze zdarzeniami występującymi w cyberprzestrzeni są jednymi z najbardziej powszechnych i realnych zagrożeń dla bezpieczeństwa współczesnego państwa. Nie ulega zatem wątpliwości, że zagadnienia zarządzania kryzysowego, informatyzacji, telekomunikacji, rozwoju usług świadczonych drogą elektroniczną, czy interoperacyjności są integralnie związane z kwestiami bezpieczeństwa teleinformatycznego i w żadnym przypadku nie mogą być traktowane rozłącznie. Stanowisko Ministra Administracji i Cyfryzacji, że można informatyzować państwo, czy chronić infrastrukturę krytyczną z pominięciem aspektów bezpieczeństwa teleinformatycznego wskazuje na ignorowanie występujących w tym obszarze ryzyk, których potencjalne konsekwencje dla funkcjonowania państwa należy ocenić jako krytyczne. **W ocenie NIK niezbędna jest zatem pilna zmiana podejścia kierownictwa najważniejszych podmiotów publicznych do zagrożeń związanych z funkcjonowaniem cyberprzestrzeni i wynikających z tego faktu nowych zadań administracji państwowej. Brak świadomości zagrożeń i ich konsekwencji w praktyce sparaliżował dotychczasową aktywność państwa w tym obszarze.**

Przypisanie zasobów do realizacji zadań związanych z ochroną cyberprzestrzeni RP

NIK negatywnie ocenia fakt, że nie zostały dotychczas podjęte żadne działania, mające na celu opracowanie założeń i wdrożenie systemu finansowania zadań związanych z bezpieczeństwem teleinformatycznym państwa. W związku ze stanowiskiem Ministra Finansów oraz przedstawicieli Kancelarii Prezesa Rady Ministrów, wyrażanym m.in. w toku prac nad „Polityką", dotyczącym konieczności „bezkosztowego" prowadzenia działań w zakresie ochrony cyberprzestrzeni, nie zostały przydzielone żadne dodatkowe środki finansowe na realizację tych

[68] Obowiązki w tym zakresie wynikały z § 4 ust. 3 rozporządzenia w sprawie planu działań przedsiębiorcy telekomunikacyjnego w sytuacjach szczególnych zagrożeń.

zadań. W toku kontroli stwierdzono natomiast, że w przypadku większości badanych jednostek, zasoby przypisane do realizacji zadań związanych z ochroną cyberprzestrzeni były całkowicie nieadekwatne i niewystarczające do efektywnego działania, i tak:

- **w MAiC nie przypisano zasobów oraz nie zbudowano potencjału kadrowego i merytorycznego pozwalającego na realne wykonywanie zadań Ministra Administracji i Cyfryzacji w zakresie koordynacji i inicjowania działań instytucji państwowych związanych z bezpieczeństwem teleinformatycznym oraz koordynacji krajowego systemu reagowania na incydenty komputerowe w cyberprzestrzeni RP. W okresie pierwszych 2 lat funkcjonowania Ministerstwa, ww. zadania były doraźnie wykonywane przez pracowników Gabinetu Politycznego Ministra, a przez większość tego okresu przez jedną osobę – Szefową Gabinetu Politycznego**. Dopiero od stycznia 2014 r., tj. po otrzymaniu pierwszego pisma NIK w ramach przygotowania niniejszej kontroli, wyznaczono komórkę merytoryczną MAiC – Wydział Unii Europejskiej i Spraw Międzynarodowych Departamentu Społeczeństwa Informacyjnego – odpowiedzialną za realizację zadań związanych z ochroną cyberprzestrzeni (początkowo nieformalnie – na podstawie polecenia wydanego przez Podsekretarza Stanu w MAiC, a formalnie od sierpnia 2014 r., na podstawie zmienionego regulaminu organizacyjnego Ministerstwa). Komórka ta nie była jednak 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 działania w obszarze bezpieczeństwa teleinformatycznego. **Przykładem niewystarczających kwalifikacji pracowników MAiC, było m.in. ustalone w trakcie kontroli przesłanie, przez jedną z ww. osób, z wykorzystaniem prywatnej, darmowej 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 RP zostały podjęte dopiero w trakcie kontroli NIK i polegały one na zatrudnieniu 2 dodatkowych pracowników, z których jedna osoba miała wykształcenie humanistyczne oraz nie posiadała (poza stażami) żadnego doświadczenia zawodowego i dopiero rozpoczęła dokształcanie w zakresie tematyki związanej m.in. z bezpieczeństwem informacji.

  Nieformalny charakter działań związanych z bezpieczeństwem cyberprzestrzeni w pierwszych latach funkcjonowania Ministerstwa, skutkował całkowitym brakiem ciągłości realizacji zadań urzędu w tym zakresie. Od momentu przejęcia zadań w styczniu 2014 r. przez Departament Społeczeństwa Informacyjnego, 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 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. Ustalono również, że pracownicy oraz Członek Kierownictwa Ministerstwa odpowiadający za realizację „Polityki" nie mieli wiedzy o trwających w ABW od kilku miesięcy pracach związanych z przygotowaniem kompleksowej metodyki szacowania ryzyka wymaganej na podstawie pkt 3.1. tego dokumentu. W związku z powyższym, pomimo otrzymania od ABW pisma

zawierającego przedmiotową metodykę, w pośpiechu, bez gruntownego rozpoznania rynku i z wyłączeniem obowiązujących w MAiC procedur udzielania zamówień publicznych, zamówiono ją równolegle u komercyjnego podmiotu zewnętrznego (szczegółowo opisano na str. 50 informacji);

- **funkcjonujące w Polsce główne państwowe zespoły CERT nie posiadały wystarczających zasobów, pozwalających na skuteczne reagowanie na incydenty dotyczące wszystkich podmiotów objętych ich zakresem oddziaływania**. W kontrolowanym okresie, zatrudnienie w rządowym Zespole CERT.GOV.PL funkcjonującym w ramach ABW, wahało się pomiędzy 12 a 14 osobami, natomiast w ocenie kierownictwa Agencji do sprawnej realizacji zadań ochrony cyberprzestrzeni administracji państwowej oraz podstawowego zakresu ochrony systemów infrastruktury krytycznej, niezbędne jest zaangażowanie w Zespole od 80 do 100 osób. Odrębny problem dla pozyskania i utrzymania w Agencji odpowiednio wykwalifikowanej kadry stanowi również system wynagradzania, który nie jest uzależniony od posiadanych kwalifikacji, czy umiejętności, a w głównej mierze wynika z regulacji prawnych określających grupy uposażenia zasadniczego oraz dodatki. W przypadku Zespołu CERT Polska, pełniącego rolę CERTu de facto narodowego, ograniczony zakres działalności wynikał z faktu, iż jest on przede wszystkim Zespołem wspomagającym konkretną działalność gospodarczą NASK, podporządkowanym interesom ekonomicznym tej instytucji. Ewentualne zwiększenie aktywności Zespołu, zgodnie ze stanowiskiem Kierownictwa NASK, mogłoby nastąpić po otrzymaniu adekwatnych środków i zasobów z budżetu państwa;
- **w jednostkach organizacyjnych Policji nie został wdrożony kompleksowy system reagowania na zagrożenia i incydenty występujące w cyberprzestrzeni oraz nie zorganizowano wewnętrznego zespołu reagowania na incydenty komputerowe, co wyjaśniano ograniczeniami kadrowymi i finansowymi**. W rezultacie, nie były badane, ani wyjaśniane incydenty występujące w jawnych systemach i sieciach teleinformatycznych Policji[69]. Ponadto, w ocenie Kierownictwa Policji, system wynagrodzeń funkcjonariuszy i pracowników cywilnych nie pozwala na pozyskanie i utrzymanie wystarczającej liczby odpowiednio wykwalifikowanych specjalistów w obszarze ochrony cyberprzestrzeni, co stwarza ryzyko niedostosowania kadr Policji do wzrastającej liczby skomplikowanych spraw z zakresu przestępczości komputerowej. Uwagi w ww. zakresie były również zgłaszane w trakcie kontroli NIK, przez Kierownictwo Zespołu CERT Polska, które wskazywało na istotne problemy komunikacyjne w zakresie współpracy z Policją i niewystarczające przygotowanie merytoryczne funkcjonariuszy zajmujących się sprawami przestępczości komputerowej;
- w resorcie obrony narodowej zbudowano złożone struktury organizacyjne przeznaczone do realizacji zadań związanych z ochroną cyberprzestrzeni obejmujące różne komórki i jednostki organizacyjne, tj. w szczególności: trójpoziomowy system reagowania na incydenty komputerowe, Pełnomocnika Ministra Obrony Narodowej do spraw Bezpieczeństwa Cyberprzestrzeni, Narodowe Centrum Kryptologii (NCK), Inspektorat Systemów Informacyjnych[70], Centrum Bezpieczeństwa Cybernetycznego Sił Zbrojnych. **W ocenie Kierownictwa MON, resort obrony narodowej nie dysponuje jednak odpowiednią liczbą specjalistów**

69 W latach 2012–2014, Biuro Łączności i Informatyki Komendy Głównej Policji otrzymało z Zespołu CERT.GOV.PL 1 807 informacji na temat zagrożeń i incydentów zidentyfikowanych w jawnych, policyjnych systemach teleinformatycznych.

70 Wypełniający zadania: administratora sieci i kluczowych usług teleinformatycznych, gestora korpusu osobowego łączności i informatyki, gestora sprzętu i oprogramowania informatycznego.

posiadających wystarczające kwalifikacje w obszarze ochrony cyberprzestrzeni – stan ukompletowania jednostek odpowiadających za bezpieczeństwo IT wynosił tylko 40%[71]. Ponadto, cały system organizacyjny resortu powołany do ochrony cyberprzestrzeni, został podporządkowany NCK – nowej jednostce organizacyjnej zajmującej się tylko jednym z aspektów bezpieczeństwa informacji jakim jest „poufność" i będącej dopiero na etapie formowania. Z ustaleń kontroli wynika, że Kierownictwo NCK napotykało na istotne problemy związane z rekrutacją wykwalifikowanego personelu (prawie półtora roku od utworzenia jednostki stan jej ukompletowania wynosił tylko 36%) oraz nie dysponowało infrastrukturą (bazą lokalową i zapleczem technologiczno-produkcyjnym) pozwalającą na rozpoczęcie efektywnej działalności. Stworzyło to, w ocenie NIK, duże ryzyko dla ciągłości działania i efektywności struktur organizacyjnych resortu powołanych do ochrony cyberprzestrzeni. Uwagi NIK dotyczyły także, podporządkowania całego systemu instytucjonalnego resortu związanego z bezpieczeństwem IT jednej osobie, będącej jednocześnie m.in. Pełnomocnikiem Ministra Obrony Narodowej do spraw Bezpieczeństwa Cyberprzestrzeni, Dyrektorem NCK oraz Przewodniczącym (i zarazem Wiceprzewodniczącym) resortowego Zespołu ds. Opracowania Projektu Założeń do Planu Obrony Cyberprzestrzeni RP. Wskazane przez NIK ryzyko, dotyczące odejścia ww. osoby z Ministerstwa, zmaterializowało się bezpośrednio po zakończeniu kontroli, w styczniu 2015 r., co skutkowało koniecznością dokonania istotnych zmian strukturalnych i kadrowych w systemie ochrony cyberprzestrzeni MON;

- w MSW, w wyniku zmian organizacyjnych i kadrowych, w okresie objętym kontrolą, uległa zmniejszeniu liczebność komórki organizacyjnej zajmującej się kwestiami bezpieczeństwa teleinformatycznego (z 10 do 3 pracowników) oraz obniżył się poziom kwalifikacji zatrudnionych w niej osób (brak osób z wykształceniem informatycznym), co w ocenie NIK miało niekorzystny wpływ na realizację zadań Ministra Spraw Wewnętrznych w zakresie ochrony cyberprzestrzeni.

NIK negatywnie ocenia fakt, iż pomimo braku wystarczających i adekwatnych zasobów do realizacji zadań związanych z ochroną cyberprzestrzeni RP, żaden z kontrolowanych podmiotów nie podjął nawet próby oszacowania środków (ludzkich, rzeczowych i finansowych) potrzebnych do efektywnego prowadzenia działań w tym obszarze. W poszczególnych jednostkach wystąpiły problemy z precyzyjnym określeniem kwoty wydatków poniesionych dotychczas na realizację zadań związanych z bezpieczeństwem teleinformatycznym, ponieważ wydatki te nie były odrębnie oznaczane i wykazywane w ewidencji księgowej. Kontrolowane jednostki nie wykonywały w ogóle 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 cyberprzestrzeni.

Stwierdzono także, że Minister Administracji i Cyfryzacji nie podjął działań mających na celu oszacowanie zasobów (ludzkich, rzeczowych i finansowych) niezbędnych do realizacji zadań związanych z wdrażaniem „Polityki" i ochroną cyberprzestrzeni RP. W Ministerstwie nie sporządzano analiz, kalkulacji, itp. będących próbą zwymiarowania tych zasobów oraz nie dysponowano nawet ogólną wiedzą na temat potrzeb i środków będących w dyspozycji poszczególnych podmiotów zaangażowanych w ochronę bezpieczeństwa teleinformatycznego państwa. Pomimo nieotrzymania informacji określonych w pkt 5 „Polityki", Minister nie podjął żadnych działań monitujących w celu

[71] Wg stanu na dzień 9 października 2014 r.

wyegzekwowania od podmiotów administracji rządowej realizacji obowiązków określonych w ww. dokumencie. Nie wydał również wytycznych dotyczących sposobu wykonania tych obowiązków, w szczególności w zakresie sposobów ewidencjonowania i szacowania wydatków na ochronę cyberprzestrzeni.

NIK ocenia jako nierzetelne, niepodjęcie przez MAiC starań w celu uzyskania środków finansowych pozwalających na wdrożenie realnych działań w obszarze ochrony cyberprzestrzeni. Poza dwoma konkretnymi przypadkami (dotyczącymi systemu wczesnego ostrzegania oraz skutków finansowych dyrektywy NIS), Minister Administracji i Cyfryzacji nie prowadził konsultacji z Ministrem Finansów, dotyczących finasowania zadań w obszarze bezpieczeństwa teleinformatycznego. Nie informował także Prezesa Rady Ministrów o ograniczeniach kadrowych i finansowych uniemożliwiających rzetelną realizację zadań MAiC związanych z wdrażaniem „Polityki" oraz koordynacją krajowego systemu reagowania na incydenty komputerowe w cyberprzestrzeni RP. Nie podjęto również działań w celu przygotowania konkretnych projektów pozwalających na uzyskanie dofinansowania tych zdań ze środków zagranicznych[72]. Z wyjaśnień Kierownictwa MAiC wynika, że zaakceptowano stanowisko Ministra Finansów dotyczące braku możliwości przeznaczenia dodatkowych nakładów na bezpieczeństwo teleinformatyczne.

Kontrola wykazała, że brak określenia źródeł finansowania i nieprzypisanie zasobów praktycznie sparaliżowały działania podmiotów państwowych w zakresie ochrony cyberprzestrzeni RP[73]. Nie ulega wątpliwości, że bezpieczeństwo teleinformatyczne (tak jak np. utrzymanie formacji ochrony bezpieczeństwa i porządku, czy też sił zbrojnych) wymaga dużych nakładów finansowych[74], adekwatnych do realizowanych zadań. Dalsze ignorowanie tego faktu, w ocenie NIK, będzie stwarzać istotne zagrożenie dla infrastruktury państwa i wykluczy możliwość skutecznego reagowania struktur państwowych na zdarzenia występujące w cyberprzestrzeni, co może pociągnąć za sobą znaczące konsekwencje, w tym finansowe.

Określenie ram prawnych systemu ochrony cyberprzestrzeni

NIK ocenia negatywnie fakt, że w Polsce nie opracowano dotychczas przepisów kompleksowo regulujących kwestie bezpieczeństwa teleinformatycznego państwa. Ze względu na brak ustawowego uregulowania krajowego systemu ochrony cyberprzestrzeni i jego uczestników, nie zostały dotychczas precyzyjnie określone obowiązki i kompetencje podmiotów państwowych związane z bezpieczeństwem teleinformatycznym. Zadania poszczególnych instytucji były rozproszone w różnych regulacjach prawnych. Wynikały one przede wszystkim z przepisów dotyczących: działów administracji rządowej, zarządzania kryzysowego, Prawa telekomunikacyjnego, informatyzacji, funkcjonowania organów porządku i bezpieczeństwa publicznego, zakresów działania poszczególnych Ministrów, a także z regulacji wewnętrznych różnych instytucji. W rezultacie, obowiązki i kompetencje poszczególnych podmiotów były niejasne, niespójne oraz realizowane bez jednolitych

---

72 Z informacji uzyskanych, w trybie art. 29 ust. 1 pkt 2 lit. f ustawy o NIK, z Ministerstwa Infrastruktury i Rozwoju wynika, że w ramach perspektywy finansowej na lata 2007–2013 nie realizowano żadnych projektów współfinansowanych ze środków zagranicznych związanych bezpośrednio z ochroną cyberprzestrzeni RP. Wskazano możliwość realizacji takich projektów w ramach Programu Operacyjnego Polska Cyfrowa na lata 2014–2020, natomiast wg stanu na dzień 25 lutego 2014 r., żadne tego typu projekty nie otrzymały jeszcze dofinansowania.

73 Dla kontrastu należy wskazać, że w ramach Narodowego Program Ochrony Cyberprzestrzeni Wielkiej Brytanii na lata 2011–2014 zaplanowano wydatki w kwocie 650 mln funtów (równolegle do wydatków ponoszonych w ramach własnych budżetów podmiotów uczestniczących w ochronie cyberprzestrzeni).

74 Analogiczne stanowisko zostało przedstawione w opracowanej dla NIK ekspertyzie zewnętrznej – Instytut Kościuszki, „Propozycja modelowych rozwiązań w zakresie budowania cyberbezpieczeństwa Polski", Kraków 2015.

ram systemowych. Przeprowadzona kontrola wykazała także, że obowiązujące obecnie, rozproszone regulacje dotyczące bezpieczeństwa teleinformatycznego, tylko w niewielkim stopniu stanowiły podstawę realnych działań związanych z ochroną cyberprzestrzeni RP. Wynikało to w szczególności z wadliwego sformułowania części przepisów oraz z braku świadomości i zrozumienia wynikających z nich obowiązków ze strony kierownictwa kontrolowanych podmiotów, i tak:

- obowiązujące regulacje dotyczące zarządzania kryzysowego, w ograniczonym zakresie były wykorzystywane do wdrożenia efektywnych mechanizmów ochrony krytycznej infrastruktury teleinformatycznej państwa. W szczególności, w oparciu o te przepisy, nie opracowano dotychczas procedur reagowania kryzysowego w sytuacjach incydentów związanych z cyberprzestrzenią (szczegółowo opisano na str. 62–65 informacji);
- ustanowiony na podstawie Działu VIIa Prawa telekomunikacyjnego[75] system zbierania przez Prezesa UKE zgłoszeń o incydentach oraz informowania o nich konsumentów i właściwych instytucji (krajowych i unijnych) był całkowicie nieskuteczny oraz nie zapewniał rzetelnej i wiarygodnej wiedzy o naruszeniach bezpieczeństwa sieci lub usług związanych z cyberprzestrzenią. Stwierdzono także, że opracowywane przez przedsiębiorców telekomunikacyjnych[76] plany działań w sytuacjach szczególnych zagrożeń, odnosiły się, co do zasady, do konwencjonalnych niebezpieczeństw i nie mogły być wykorzystywane jako analiza ryzyka oraz procedury reagowania kryzysowego związane z bezpieczeństwem teleinformatycznym (szczegółowo opisano na str. 57–58 oraz 65 informacji);
- podmioty administracji rządowej nie realizowały obowiązków kontrolnych wymienionych w art. 25 ust. 1 pkt 3 ustawy o informatyzacji, dotyczących m.in. weryfikacji przestrzegania wymogów bezpieczeństwa systemów teleinformatycznych wykorzystywanych do realizacji zadań publicznych (szczegółowo opisano na str. 60–62 informacji).

Ustalenia kontroli wykazały, że pomimo opisanych powyżej istotnych braków oraz nieprzestrzegania przepisów dotyczących ochrony cyberprzestrzeni, nie były dotychczas prowadzone żadne prace legislacyjne mające na celu unormowanie zagadnień związanych z bezpieczeństwem teleinformatycznym państwa. Nie przeprowadzono inwentaryzacji rozproszonych przepisów związanych z cyberbezpieczeństwem oraz nie zdefiniowano pożądanych kierunków zmian legislacyjnych. Nie przygotowano nawet założeń aktu normatywnego określającego strukturę krajowego systemu ochrony cyberprzestrzeni i jego uczestników. Nieliczne propozycje zmian legislacyjnych zgłaszane w tym zakresie przez podmioty takie jak UKE, RCB i Policja[77], napotykały bierność i brak rzetelnego rozpatrzenia ze strony organów nadrzędnych, tj. Ministra Administracji i Cyfryzacji oraz Ministra Spraw Wewnętrznych.

---

75 Art. 175a – 175e Prawa telekomunikacyjnego.

76 Na podstawie art. 176a Prawa telekomunikacyjnego.

77 Zgłaszane propozycje zmian legislacyjnych związanych z ochroną cyberprzestrzeni dotyczyły: zmiany art. 175a ust. 1 Prawa telekomunikacyjnego poprzez nałożenie na przedsiębiorców telekomunikacyjnych bezwzględnego obowiązku informowania o naruszeniach według określonego kryterium (progów zgłoszeń) oraz wypracowania jednej, wspólnej dla wszystkich przedsiębiorców metody szacowania liczby użytkowników dotkniętych naruszeniem (UKE), nowelizacji zarządzenia nr 74 Prezes Rady Ministrów w sprawie wykazu przedsięwzięć i procedur systemu zarzadzania kryzysowego, dotyczącej m.in. ustanowienia czterech stopni alarmowych, wprowadzanych w razie wystąpienia zagrożeń o charakterze terrorystycznym lub sabotażowym dla systemów teleinformatycznych administracji państwowej oraz infrastruktury krytycznej (RCB), zmiany ustawy o świadczeniu usług drogą elektroniczną polegającej m.in. na zobowiązaniu przedsiębiorców świadczących usługi drogą elektroniczną do zatrzymywania i przechowywania danych o nawiązanych połączeniach, w tym bezpłatnego udostępniania tych danych Policji (Komendant Główny Policji).

Stwierdzono także, że Minister Administracji i Cyfryzacji, który zgodnie z pkt 3.3 „Polityki" był zobowiązany do przygotowania i niezwłocznego zainicjowania prac legislacyjnych związanych z budową krajowego systemu ochrony cyberprzestrzeni, nie podjął żadnych działań w tym zakresie. Powyższe wynikało w szczególności, z przyjęcia przez Kierownictwo Ministerstwa założenia, że budowa krajowych struktur odpowiadających za bezpieczeństwo teleinformatyczne i opracowanie stosownych regulacji w tym obszarze, powinny być całkowicie wstrzymane do czasu wejścia w życie dyrektywy NIS, która określi konkretne rozwiązania dla całej Unii Europejskiej. W związku z powyższym, aktywność Ministra w zakresie działań legislacyjnych ograniczyła się do udziału w pracach instytucji UE, związanych z przygotowaniem projektu ww. dyrektywy. W trakcie 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.

W ocenie NIK, stanowisko Ministra Administracji i Cyfryzacji dotyczące niezasadności budowy krajowych rozwiązań instytucjonalnych w zakresie bezpieczeństwa teleinformatycznego do czasu wejścia w życie regulacji unijnych jest błędne i nie uwzględnia postępującego wzrostu zagrożeń w obszarze cyberprzestrzeni dla infrastruktury państwa i obywateli. Z wyników analizy przedkontrolnej[78] oraz niezależnej ekspertyzy przygotowanej dla NIK[79] wynika jednoznacznie, że większość państw europejskich podjęła już systemowe działania w zakresie bezpieczeństwa teleinformatycznego, a Polska jest jednym z niewielu krajów Europy, który swoje działania w tym zakresie całkowicie uzależnił od inicjatyw zewnętrznych. Należy podkreślić, że w związku ze sprzecznymi interesami państw członkowskich UE, na chwilę obecną nie można nawet określić przewidywanej daty wejścia w życie dyrektywy NIS, a ponadto okres implementacji tej regulacji ma wynosić 2,5 roku. Dotychczasowe prace prowadzone w instytucjach UE nad projektem dyrektywy wykazały także duże ryzyko, że będzie ona miała ogólny charakter i tylko w niewielkim stopniu będzie oddziaływać na poziom bezpieczeństwa teleinformatycznego poszczególnych krajów. W związku z powyższym, w ocenie NIK, istnieje pilna potrzeba zainicjowania prac legislacyjnych, w celu przyjęcia kompleksowych regulacji określających strukturę, zasady funkcjonowania oraz obowiązki i kompetencje poszczególnych uczestników krajowego systemu ochrony cyberprzestrzeni.

Określenie wskaźników realizacji zadań związanych z ochroną cyberprzestrzeni RP

Kontrola wykazała, że działania podmiotów państwowych w zakresie ochrony cyberprzestrzeni były prowadzone w sposób niespójny, bez rzetelnego planowania, przygotowania i jednolitej wizji systemowej.

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. W celu uzupełnienia ww. dokumentu, w pkt 6. i 6.3. „Polityki", zawarto specjalną procedurę, obejmującą dwa etapy, tj.:

[78] W ramach analizy przedkontrolnej NIK wystąpiła m.in. do najwyższych organów kontrolnych 12 państw z prośbą o przekazanie informacji na temat funkcjonujących w tych krajach rozwiązań systemowych w zakresie ochrony cyberprzestrzeni.

[79] Instytut Kościuszki, „Propozycja modelowych rozwiązań w zakresie budowania cyberbezpieczeństwa Polski", Kraków 2015.

- opracowanie przez poszczególne podmioty zaangażowane w ochronę cyberprzestrzeni jednostkowych wskaźników realizacji zadań (w ciągu roku od wejścia w życie „Polityki");
- opracowanie przez Ministra Administracji i Cyfryzacji globalnych, zagregowanych wskaźników realizacji „Polityki" (po przeprowadzeniu szacowania ryzyka).

Ustalono, że podmioty administracji rządowej nie realizowały obowiązków wynikających z powyższych punktów „Polityki", polegających na przekazaniu Ministrowi Administracji i Cyfryzacji, w ciągu roku od przyjęcia tego dokumentu, informacji na temat przyjętych i osiągniętych wskaźników realizacji działań związanych z ochroną cyberprzestrzeni. **W skontrolowanych jednostkach[80] nie przeprowadzono rzetelnych analiz pozwalających na zdefiniowanie ich zadań w obszarze bezpieczeństwa teleinformatycznego państwa oraz przypisanych do nich mierników**. Obowiązek dotyczący przekazania wskaźników do MAiC, został wykonany tylko przez Dyrektora RCB, natomiast zdefiniowane przez niego zadania i mierniki dotyczyły wyłącznie ochrony wewnętrznych zasobów teleinformatycznych Urzędu – całkowicie pominięto podstawowe zadania RCB, związane z ochroną krytycznej infrastruktury teleinformatycznej państwa. Pomimo nieotrzymania informacji wymaganych na podstawie „Polityki", Minister Administracji i Cyfryzacji nie podjął żadnych działań monitujących w celu wyegzekwowania realizacji obowiązków określonych w pkt 6. i 6.3. tego dokumentu. W MAiC nie rozpoczęto również prac zmierzających do przygotowania globalnych, zagregowanych wskaźników realizacji zadań wymienionych w „Polityce". Brak aktywności i wytycznych ze strony Ministra Administracji i Cyfryzacji, były wskazywane przez kierownictwo kontrolowanych jednostek, jako jedna z głównych przyczyn niezrealizowania określonych w „Polityce" obowiązków, dotyczących zdefiniowania mierników realizacji zadań związanych z ochroną cyberprzestrzeni.

NIK negatywnie ocenia również fakt, że do końca okresu objętego kontrolą, nie zostały opracowane żadne, przewidziane w „Polityce" projekty szczegółowe[81], precyzujące zakres i formy realizacji poszczególnych, wskazanych w tym dokumencie zadań dotyczących bezpieczeństwa teleinformatycznego państwa. Należy podkreślić, że Minister Administracji i Cyfryzacji, odpowiadający za wdrażanie „Polityki", nie potrafił nawet wskazać kto odpowiada za przygotowanie i realizację projektów szczegółowych, ani jaka powinna być ich forma i zawartość. Minister nie podejmował żadnych działań w celu opracowania projektów, stanowiących uszczegółowienie poszczególnych działań wymienionych w „Polityce" oraz nie dysponował wiedzą, czy i jakie projekty są realizowane przez inne podmioty zobowiązane do wdrażania tego dokumentu. **W rezultacie, instytucje państwowe nie miały precyzyjnie zdefiniowanych zadań w obszarze bezpieczeństwa teleinformatycznego, a ich ewentualna aktywność w tym obszarze była wynikiem jedynie inicjatywy kierownictwa poszczególnych jednostek oraz ich indywidulanej interpretacji niejasnych zapisów „Polityki"**.

[80] Z wyjątkiem MON, w którym określono mierniki realizacji zadań dotyczących bezpieczeństwa resortowych sieci i systemów teleinformatycznych.

[81] 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".

Koordynacja działań związanych z ochroną cyberprzestrzeni RP

W ocenie NIK, podmioty administracji państwowej nie prowadziły rzetelnej i efektywnej współpracy w zakresie realizacji zadań związanych z ochroną cyberprzestrzeni RP. Nie zostały także wdrożone skuteczne mechanizmy koordynacji działań w tym obszarze.

Kontrola wykazała w szczególności, że nie został powołany przez Prezesa Rady Ministrów, przewidziany w pkt 3.4.1 „Polityki", międzyresortowy Zespół mający wspierać Ministra Administracji i Cyfryzacji w koordynacji działań związanych z bezpieczeństwem cyberprzestrzeni. MAiC pierwotnie wnioskowało o powołanie ww. Zespołu i przygotowało projekt zarządzenia w tej sprawie (przewidujący m.in. przedkładanie Radzie Ministrów wyników prac oraz okresowych sprawozdań z działalności Zespołu), natomiast w wyniku nieoficjalnych uzgodnień między ówczesnym Ministrem Administracji i Cyfryzacji – Panem Rafałem Trzaskowskim, a Kierownictwem Kancelarii Prezesa Rady Ministrów, zrezygnowano z powołania odrębnego organu pomocniczego Rady Ministrów zajmującego się tematyką ochrony cyberprzestrzeni. Szef Kancelarii Prezesa Rady Ministrów wyjaśnił[82], że decyzja ta wynikała z dążenia do ograniczenia liczby zespołów międzyresortowych oraz z przekonania o braku racjonalności powołania odrębnego Zespołu odpowiadającego za ww. zagadnienia. W ocenie NIK, przedstawiona argumentacja świadczy o nieprzykładaniu należytej wagi do kwestii bezpieczeństwa teleinformatycznego państwa. Należy zauważyć, że w chwili obecnej funkcjonuje około 20 organów pomocniczych Rady Ministrów[83] zajmujących się zagadnieniami prawnymi, ekonomicznymi i społecznymi o różnej wadze. Wśród ww. organów można wymienić Stały Komitet Rady Ministrów, Komitet Sterujący ds. Projektu Terminal LNG w Świnoujściu, ale także np. Zespół ds. obchodów 600-lecia nawiązania polsko-tureckich stosunków dyplomatycznych. W ocenie NIK, nie ulega natomiast wątpliwości, że uwzględniając dynamikę wzrostu i „powszechność" zagrożeń występujących w cyberprzestrzeni, przedmiotowy obszar wymaga pogłębionej współpracy i koordynacji działań różnych podmiotów państwowych. Rezygnacja z powołania Zespołu pomocniczego Rady Ministrów, ograniczyła w wysokim stopniu bieżący udział w działaniach związanych z ochroną cyberprzestrzeni Rady Ministrów i Prezesa Rady Ministrów odpowiadających, zgodnie z Konstytucją RP, za bezpieczeństwo państwa oraz posiadających uprawnienia w zakresie egzekwowania obowiązków od poszczególnych ministrów i szefów urzędów centralnych.

W miejsce Zespołu wymienionego w pkt 3.4.1 „Polityki", Minister Administracji i Cyfryzacji[84], powołał podmiot o znacznie niższej randze, tj. „Zespół zadaniowy do spraw bezpieczeństwa cyberprzestrzeni Rzeczypospolitej Polskiej", będący zespołem zadaniowym Komitetu Rady Ministrów do spraw Cyfryzacji[85]. Przedmiotowa decyzja była niezgodna z uchwałą Rady Ministrów w sprawie przyjęcia „Polityki", w zakresie formy prawnej ww. Zespołu oraz w sposób nieuprawniony wydłużyła o 60 dni termin realizacji kluczowego zadania określonego w pkt 3.4.1 „Polityki", dotyczącego opracowania

82 Szef Kancelarii Prezesa Rady Ministrów – Pan Jacek Cichocki, udzielił wyjaśnień na pytanie zadane w tej sprawie Prezesowi Rady Ministrów.

83 Wg stanu na dzień 25 marca 2015 r.

84 Działając jako Przewodniczący Komitetu Rady Ministrów do spraw Cyfryzacji.

85 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.

„Planu działań w zakresie zapewnienia bezpieczeństwa cyberprzestrzeni RP" (zwanego dalej „Planem działań"). W decyzji nie określono trybu zatwierdzania wyników prac Zespołu, w związku z czym przygotowany przez niego „Plan działań" oraz inne wytyczne mogą nie uzyskać charakteru wiążącego i będą stanowić tylko ogólną rekomendację dla pozostałych instytucji publicznych.

Ustalono też, że dotychczasowa współpraca podmiotów uczestniczących w pracach Zespołu była nierzetelna, nieefektywna i nie wpływała realnie na podnoszenie poziomu bezpieczeństwa teleinformatycznego państwa, i tak:

- „Zespół zadaniowy do spraw bezpieczeństwa cyberprzestrzeni Rzeczypospolitej Polskiej" został powołany dopiero rok od wejścia w życie „Polityki" (w dniu 13 czerwca 2014 r.), a do końca okresu objętego kontrolą odbyło się tylko jedno jego posiedzenie, pomimo że zgodnie z decyzją powołującą, posiedzenia Zespołu powinny się odbywać, co najmniej raz na kwartał;
- do końca kontroli nie zostało zrealizowane podstawowe zadanie ww. Zespołu, dotyczące przygotowania w terminie do dnia 13 września 2014 r. „Planu działań w zakresie zapewnienia bezpieczeństwa cyberprzestrzeni RP"[86]. Nie rozpoczęto także nawet prac związanych z realizacją pozostałych, istotnych zadań Zespołu dotyczących m.in. opracowania propozycji działań mających na celu ochronę systemów teleinformatycznych i usług przed cyberatakami oraz propozycji standardów bezpieczeństwa dla systemów teleinformatycznych jednostek administracji rządowej (zgodnie z decyzją powołującą Zespół, przedmiotowe zadania powinny były zostać wykonane do dnia 13 grudnia 2014 r.);
- dokumentacja przekazywana przez poszczególne instytucje uczestniczące w pracach Zespołu, jako wkłady do „Planu działań" w wielu przypadkach była niekompletna[87], nierzetelnie przygotowana oraz przedstawiona w innej szczegółowości, niż wymagana przez MAiC (np. Dyrektor Narodowego Centrum Kryptologii przekazał propozycje działań w układzie całkowicie odbiegającym od wytycznych MAiC). Część podmiotów przekazała dane odnoszące się wyłącznie do wewnętrznych systemów teleinformatycznych, bez uwzględnienia wkładu tych instytucji w krajowy system ochrony cyberprzestrzeni (Minister Spraw Wewnętrznych, Minister Sprawiedliwości, Komendant Główny Policji, Minister Zdrowia), a niektóre organy państwowe w ogóle nie wywiązały się z obowiązku przekazania wkładów do MAiC (Minister Edukacji Narodowej, Generalny Inspektor Ochrony Danych Osobowych).

Minister Administracji i Cyfryzacji nierzetelnie i z opóźnieniem przygotowywał prace ww. Zespołu oraz nie podejmował żadnych działań w celu wyegzekwowania od pozostałych jego członków przekazania wymaganej dokumentacji lub uzupełnienia nienależycie przygotowanych materiałów. Powyższe wynikało zarówno z braku przygotowania organizacyjnego i kadrowego MAiC do koordynacji działań związanych z ochroną cyberprzestrzeni (szczegółowo opisano na str. 41 informacji), jak również z braku uprawnień do egzekwowania jakichkolwiek obowiązków od innych ministrów, szefów urzędów centralnych i kierownictwa podmiotów publicznych. W związku z powyższym, NIK oceniła także jako nierzetelne, zaakceptowanie przez Ministra Administracji i Cyfryzacji, odstąpienia od powołania Zespołu pomocniczego Rady Ministrów określonego w pkt 3.4.1. „Polityki", który mógłby stanowić faktyczne forum koordynacji działań organów państwowych związanych z ochroną cyberprzestrzeni RP.

86 W MAiC opracowano wstępny projekt tego dokumentu, który miał być przedłożony członkom Zespołu na kolejnym posiedzeniu.

87 M.in. w większości przypadków podmioty nie wskazywały zasobów (ludzkich, finansowych i rzeczowych) niezbędnych do realizacji zadań zgłaszanych do „Planu działań".

3.2.2. Szacowanie ryzyk związanych ze zdarzeniami występującymi w cyberprzestrzeni

Do końca kontroli nie przeprowadzono rzetelnej i kompleksowej analizy ryzyk związanych ze zdarzeniami występującymi w cyberprzestrzeni. Podejmowano różne próby oszacowania ryzyka w tym obszarze (m.in. w oparciu o przepisy dotyczące zarządzania kryzysowego oraz postanowienia „Polityki"), natomiast ze względu na brak komplementarności tych działań i ich nienależyte przygotowanie, osiągnięte rezultaty nie pozwoliły na prawidłowe określenie podstawowych niebezpieczeństw dla teleinformatycznej infrastruktury państwa oraz metod zarządzania tymi zagrożeniami.

Kontrola wykazała w szczególności, że nie zostało rzetelnie przygotowane i zrealizowane zadanie wymienione w pkt 3.1 „Polityki", dotyczące oszacowania przez jednostki administracji rządowej ryzyka związanego z funkcjonowaniem cyberprzestrzeni. Ustalono, że Minister Administracji i Cyfryzacji, przez okres ponad pół roku od wejścia w życie „Polityki" nie podjął żadnych działań w celu przygotowania analizy ryzyka za 2013 r., a czynności mające na celu wytworzenie metodyki niezbędnej do wykonania tego zadania, zostały podjęte dopiero pod koniec stycznia 2014 r., tj. w momencie, w którym analiza ryzyka powinna być już zakończona. MAiC nie przeprowadziło także żadnych konsultacji z innymi administratorami i użytkownikami cyberprzestrzeni, pozwalających na wykorzystanie doświadczeń tych podmiotów oraz opracowanie poprawnej merytorycznie i skutecznej metodologii szacowania ryzyka. W szczególności nie podjęto współpracy z ABW oraz z Zespołem CERT.GOV.PL., posiadającym specjalistyczną wiedzę na temat zagrożeń i incydentów teleinformatycznych. **Pracownicy i Członkowie Kierownictwa Ministerstwa nie dysponowali nawet wiedzą na temat prac prowadzonych od kilku miesięcy przez ABW nad projektem kompleksowej metodyki szacowania ryzyka dla podmiotów administracji państwowej. W rezultacie, pomimo otrzymania od ABW pisma zawierającego przedmiotową metodykę, zamówiono ją równolegle u komercyjnego podmiotu zewnętrznego**[88]. Nie dokonano przy tym gruntownego rozpoznania rynku, a Kierownictwo i pracownicy Ministerstwa nie byli w stanie ocenić jakości merytorycznej zakupionego i wykorzystywanego opracowania. Przeprowadzona analiza wykazała natomiast istotne braki zakupionej przez MAiC metodyki, polegające na nieokreśleniu precyzyjnych (porównywalnych) kryteriów identyfikacji krytycznych zasobów teleinformatycznych, które miały być objęte analizą w poszczególnych podmiotach. Powyższe, w ocenie NIK, utrudniło agregację danych z szacowania ryzyka oraz zaplanowanie adekwatnych i wspólnych dla instytucji państwowych metod przeciwdziałania i reagowania na zagrożenia. W MAiC nie opracowano również wykazu instytucji zobowiązanych do wdrażania „Polityki", w związku z czym Minister Administracji i Cyfryzacji, odpowiadający za koordynację procesu szacowania ryzyka, nie dysponował precyzyjną wiedzą na temat liczby i rodzaju podmiotów administracji rządowej (w szczególności wchodzących w skład administracji zespolonej i niezespolonej), zobowiązanych do wykonania tego zadania.

W ocenie NIK, nierzetelna była również współpraca podmiotów państwowych w zakresie szacowania ryzyka cyberprzestrzeni oraz koordynacja tego procesu przez MAiC. Stwierdzono bowiem, że część podmiotów administracji rządowej (w tym organy administracji zarządzające kluczowymi zasobami teleinformatycznymi państwa, takie jak: Minister Spraw Wewnętrznych, Minister Spraw Zagranicznych, Minister Sprawiedliwości, Minister Zdrowia, Prezes Urzędu Lotnictwa Cywilnego) nie wywiązała się z obowiązku określonego w pkt 3.1 „Polityki", tj. nie

[88] Wydatki na zakup metodyki wyniosły 3,7 tys. zł., a wskazany w umowie termin realizacji zamówienia – 4 dni.

przekazała Ministrowi Administracji i Cyfryzacji sprawozdań z analizy ryzyka. W przypadku niektórych podmiotów sprawozdania były niekompletne, zawierały błędy, zostały sporządzone w oparciu o inną metodykę i na niewłaściwym formularzu oraz zostały przekazane z opóźnieniem (np. sprawozdanie Komendanta Głównego Policji oraz sprawozdanie Ministra Administracji i Cyfryzacji w zakresie własnych zasobów informatycznych[89]). Ze względu na ograniczone zasoby komórki organizacyjnej MAiC odpowiadającej za zagadnienia cyberprzestrzeni, nie pozwalające na rzetelną analizę wszystkich otrzymanych materiałów, Minister Administracji i Cyfryzacji nie występował z monitami do podmiotów, które nie zrealizowały obowiązków z zakresu szacowania ryzyka lub przesłały niekompletne (błędnie przygotowane) sprawozdania. Powyższe uniemożliwiło agregację tych danych oraz opracowanie spójnych i kompletnych wyników szacowania ryzyka dla całej administracji państwowej. Do końca kontroli nie została również opracowana metodyka szacowania ryzyka za 2014 r., co m.in. może skutkować opóźnieniem w realizacji tego zadania w roku kolejnym[90].

Należy również wskazać, że niezależnie od opisanych powyżej nieprawidłowości, ustanowiony na podstawie pkt 3.1. „Polityki" mechanizm szacowania ryzyka związanego z funkcjonowaniem cyberprzestrzeni jest wadliwy i niekompletny, co wynika z faktu ograniczenia obowiązywania tego dokumentu, tylko do instytucji administracji rządowej. W opinii NIK, konieczne jest wprowadzenie obowiązku cyklicznego przeprowadzania analiz ryzyka z zakresu bezpieczeństwa IT, obejmującego co najmniej operatorów infrastruktury krytycznej oraz podmioty administracji państwowej (w tym jednostki samorządu terytorialnego)[91]. Powyższe, pozwoliłoby na uzyskanie rzetelnych informacji o zagrożeniach dla kluczowej teleinformatycznej infrastruktury państwa oraz zaplanowanie adekwatnych metod zarządzania tymi zagrożeniami.

Ustalono natomiast, że do czasu kontroli NIK, Kierownictwo RCB i MAiC nie podejmowało współpracy w celu zapewnienia spójności procesów zarządzania kryzysowego i ochrony cyberprzestrzeni, w tym w szczególności poprzez zapewnienie porównywalności i komplementarności metodyk analizy ryzyka wykorzystywanych przez te podmioty oraz wyników identyfikacji kluczowych, krajowych zasobów teleinformatycznych przeprowadzanej przez RCB i MAiC. W sporządzanych przez RCB cyklicznych raportach o zagrożeniach bezpieczeństwa narodowego, zagrożenia związane z cyberprzestrzenią opisywane były w sposób ogólny i ramowy, co wynikało m.in. z braku wytycznych ze strony MAiC oraz nierzetelnego przygotowania raportu cząstkowego Ministra Administracji i Cyfryzacji (szczegółowo opisano na str. 39 informacji). Uzgodnienia dotyczące określenia możliwych ram współpracy między RCB a MAiC, m.in. w zakresie komplementarności wykorzystywanych metodyk szacowania ryzyka, zostały rozpoczęte dopiero w trakcie niniejszej kontroli NIK. Propozycje dotyczące ww. zagadnień zostały zgłoszone przez Dyrektora RCB do „Planu działań w zakresie zapewnienia bezpieczeństwa cyberprzestrzeni RP".

89 Sprawozdanie z analizy ryzyka dla systemów teleinformatycznych MAiC zostało sporządzone dopiero po otrzymaniu pisma kontrolującego w ww. sprawie (tj. z półrocznym opóźnieniem), a ponadto nie było ono w pełni zgodne z metodyką i wzorem przekazanymi przez Ministra Administracji i Cyfryzacji innym podmiotom.

90 Czynności kontrolne zakończono w dniu 5 grudnia 2014 r., natomiast sprawozdania z szacowania ryzyka za 2014 r., zgodnie z pkt 3.1 „Polityki", powinny zostać przekazane do MAiC w terminie do dnia 31 stycznia 2015 r.

91 Analogiczne stanowisko zostało przedstawione w opracowanej dla NIK ekspertyzie zewnętrznej – Instytut Kościuszki, „Propozycja modelowych rozwiązań w zakresie budowania cyberbezpieczeństwa Polski", Kraków 2015.

NIK ustaliła, że w ramach analizy zagrożeń związanych z cyberprzestrzenią nie zostały również wykorzystane wyniki zleconego audytu wewnętrznego, dotyczącego bezpieczeństwa teleinformatycznego, przeprowadzonego na polecenie Prezesa Rady Ministrów, w okresie wrzesień – październik 2013 r., w 314 jednostkach administracji państwowej.

Założenia merytoryczne i organizacyjne ww. 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. Stwierdzono natomiast, że 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 ww. audytu zleconego. W MAiC opracowano tylko – w oparciu o elektroniczne dane zagregowane przez Ministerstwo Finansów – wstępne, sumaryczne zestawienie, wybranych odpowiedzi z poszczególnych ankiet audytowych. Nie przeprowadzono przy tym żadnej analizy obszernej dokumentacji źródłowej z audytu wewnętrznego – obejmującej 19 kartonów: ankiet, arkuszy z wyjaśnieniami oraz opinii, wniosków i rekomendacji przygotowanych przez audytorów z poszczególnych jednostek, a także elektroniczne bazy danych zawierające np. informacje dotyczące systemów teleinformatycznych wykorzystywanych przez podmioty państwowe. To przygotowane pobieżnie, wstępne zestawienie danych z audytu zostało przedstawione podczas pierwszego posiedzenia „Zespołu zadaniowego do spraw bezpieczeństwa cyberprzestrzeni Rzeczypospolitej Polskiej".

NIK oceniła jako nierzetelne, brak kompleksowego wykorzystania przez Ministra Administracji i Cyfryzacji wyników ww. audytu. W związku z upływem ponad roku od badań audytowych, dopuszczono do dezaktualizacji uzyskanych w ich wyniku informacji i ograniczono możliwość ich realnego wykorzystania w ramach planowania i realizacji działań związanych z ochroną cyberprzestrzeni RP. **Powyższe świadczy także o rażąco niegospodarnym zarządzaniu zasobami, ponieważ w praktyce zmarnowano wyniki skomplikowanej i długotrwałej pracy kilkuset osób – audytorów wewnętrznych oraz pracowników MF i MAiC zaangażowanych w zorganizowanie i przeprowadzenie audytu zleconego**.

W opinii NIK, brak wykorzystania wyników audytu dotyczącego bezpieczeństwa teleinformatycznego, wskazuje również na niewystarczające zaangażowanie w realizację zadań związanych z ochroną cyberprzestrzeni najwyższego kierownictwa administracji rządowej. Ustalono bowiem, że Prezes Rady Ministrów, który był inicjatorem tego audytu, pomimo nieotrzymania jego wyników, nie podjął żadnych działań w celu wyegzekwowania od Ministra Administracji i Cyfryzacji sporządzenia i przekazania zbiorczego sprawozdania audytowego. Na zadane w tej sprawie Prezesowi Rady Ministrów pytanie odpowiedział Szef Kancelarii Prezesa Rady Ministrów, który wyjaśnił, iż nie podjęto działań w tym zakresie, ponieważ to Minister Administracji i Cyfryzacji odpowiada za realizację zadań związanych z ochroną cyberprzestrzeni. Wskazał również, że koordynacja audytu wewnętrznego należy do Ministra Finansów.

3.2.3. Realizacja zadań związanych z ochroną cyberprzestrzeni

System reagowania na incydenty w cyberprzestrzeni

Kontrola NIK wykazała, że w Polsce nie funkcjonuje krajowy system reagowania na incydenty komputerowe, a przyjęte w tym zakresie zapisy „Polityki" są martwe i nieegzekwowane w praktyce. W kontrolowanym obszarze stwierdzono przykłady dobrych praktyk – powołanie i utrzymywanie przez niektóre podmioty zespołów CERT – co jednak, w ocenie NIK, nie rekompensowało braku systemowych działań państwa w tym zakresie.

Na podstawie pkt 4.2 „Polityki", Rada Ministrów ustanowiła Krajowy System Reagowania na Incydenty Komputerowe w Cyberprzestrzeni RP obejmujący:

- Poziom I – poziom koordynacji – zadania przypisano ministrowi właściwemu ds. informatyzacji;
- Poziom II – poziom reagowania na incydenty komputerowe – zadania przypisano zespołom reagowania na incydenty komputerowe;
- Poziom III – poziom realizacji – zadania przypisano administratorom odpowiadającym za poszczególne systemy teleinformatyczne funkcjonujące w cyberprzestrzeni.

W „Polityce", zaplanowano również rozbudowę zespołów reagowania na incydenty komputerowe, unifikację ich zakresów obowiązków i procedur reagowania (pkt 3.6.2 i 3.6.5) oraz budowę systemu wymiany informacji między różnymi zespołami (pkt 4.2 – 4.3).

W ramach kontroli, szczegółowym badaniem objęto funkcjonowanie 3 państwowych zespołów reagowania na incydenty komputerowe, powołanych przez ABW, NASK i MON[92]. Ustalono, że każdy z tych zespołów działa niezależnie, na rzecz odrębnej grupy użytkowników cyberprzestrzeni, i tak:

- **Zespół CERT.GOV.PL**, powołany w Departamencie Bezpieczeństwa Teleinformatycznego ABW, obejmujący swoim działaniem użytkowników z administracji publicznej. Informacja o jego powołaniu została opublikowana w Internecie. Zakresem działania Zespołu są wszystkie systemy informatyczne funkcjonujące w domenie „gov.pl" oraz pozostałe, należące do polskiej infrastruktury krytycznej. Misją Zespołu jest wytworzenie, utrzymywanie i wykorzystywanie zdolności do reagowania na incydenty bezpieczeństwa, mające miejsce w tych domenach oraz prowadzenie działań zapobiegających takim incydentom. CERT.GOV.PL nie wykonywał innych działań i usług wykraczających poza określony powyżej zakres, w szczególności nie realizował zadań na rzecz podmiotów prywatnych (spoza infrastruktury krytycznej) oraz nie pełnił roli krajowego punktu kontaktowego do spraw wymiany informacji z innymi zespołami. CERT.GOV.PL nie był członkiem żadnej organizacji międzynarodowej zrzeszającej zespoły reagowania. Nie uczestniczył również w procesach identyfikowania polskiej infrastruktury krytycznej, szacowania ryzyk oraz opracowywania planów ciągłości działania w tym obszarze. W przypadku wystąpienia sytuacji kryzysowej, Zespół został wskazany przez Szefa ABW jako właściwy w zakresie przyjmowania zgłoszeń incydentów bezpieczeństwa teleinformatycznego wykrywanych w systemach teleinformatycznych polskiej infrastruktury krytycznej. Zespół posługuje się opracowaną samodzielnie klasyfikacją zagrożeń, podatności oraz zbiorem procedur określających sposoby obsługi poszczególnych typów incydentów. W latach

[92] Poza trzema ww. państwowymi zespołami CERT, w Polsce funkcjonują prywatne zespoły reagowania na incydenty komputerowe działające w ramach poszczególnych firm, np. CERT Orange Polska lub świadczące usługi z zakresu bezpieczeństwa teleinformatycznego.

2012–2014[93], CERT.GOV.PL obsłużył 11 969 incydentów dotyczących głównie naczelnych i centralnych organów administracji państwowej. Incydenty te nie były klasyfikowane pod kątem istotności. W kontrolowany okresie zatrudnienie w Zespole wahało się pomiędzy 12 a 14 osobami, a informacje o kosztach funkcjonowania nie były upubliczniane. W ocenie ABW, do sprawnej realizacji zadań ochrony cyberprzestrzeni administracji państwowej oraz podstawowego zakresu odnoszącego się do systemów polskiej infrastruktury krytycznej, niezbędne jest zaangażowanie w Zespole od 80 do 100 osób. CERT.GOV.PL dysponuje danymi kontaktowymi do administratorów systemów teleinformatycznych z około 400 instytucji oraz danymi kontaktowymi ponad 170 osób wskazanych przez operatorów infrastruktury krytycznej. Przeprowadzona w trakcie kontroli weryfikacja tych danych kontaktowych wykazała jednak ich niską jakość i w wielu przypadkach brak aktualności;

- **Zespół CERT Polska**, powołany w ramach struktury organizacyjnej NASK, obejmujący swoim działaniem przede wszystkim klientów i użytkowników sieci NASK, a w ramach posiadanych sił i środków również użytkowników innych sieci w domenie „pl.", w szczególności w zakresie incydentów o istotnym znaczeniu – niosących za sobą straty dla zaatakowanych (głównie finansowe). Oprócz bezpośredniego reagowania na incydenty, Zespół prowadzi również stałą analizę aktualnych zagrożeń i podatności dostosowując do nich swoje metody działania. Wieloletnia obecność Zespołu CERT Polska na arenie międzynarodowej (powiązana z brakiem innych polskich przedstawicieli) spowodowała, że w wielu sytuacjach, mając na względzie ważny interes społeczny, Zespół podejmował rolę polskiego CERTu narodowego. Starał się on, w ramach posiadanych zasobów, wypełnić lukę w członkostwie w międzynarodowych organizacjach i wspólnych przedsięwzięciach. Powyższe rozwiązanie jest jednak, w ocenie kierownictwa NASK jedynie tymczasowym – Zespół w obecnej sytuacji prawnej i ekonomicznej nie planuje podejmowania kroków dla potwierdzenia swojego de facto narodowego charakteru. NASK i zespół CERT Polska nie uczestniczył formalnie w procesach szacowania ryzyka związanego ze zdarzeniami występującymi w cyberprzestrzeni, realizowanych przez inne podmioty państwowe. Zespół CERT Polska opiera stosowaną przez siebie klasyfikację incydentów na publicznej wersji opracowanej w ramach projektu eCSIRT.net. W Zespole została opracowana jedna procedura obsługi incydentów – jej zastosowanie nie jest związane z rodzajem lub wagą incydentu. W latach 2012-2013 pracownicy Zespołu CERT Polska obsłużyli bezpośrednio 2 301 incydentów, z których 8 uznano za poważne. W trakcie kontroli, w CERT Polska było zatrudnionych 16 osób. Zespół CERT Polska nie dysponuje danymi kontaktowymi pełnomocników do spraw bezpieczeństwa powołanych w jednostkach administracji rządowej oraz nie gromadzi w sposób scentralizowany danych kontaktowych administratorów systemów teleinformatycznych, które pozwalają na wymianę informacji i bieżące koordynowanie działań w sytuacji zagrożenia lub wystąpienia incydentu. W trakcie kontroli zidentyfikowano trzy rozproszone źródła takich danych obejmujące łącznie 180 kontaktów. Nie podlegały one jednak żadnej selekcji ani weryfikacji;
- **Zespół MIL-CERT.PL**, powołany jako element Systemu Reagowania na Incydenty Komputerowe resortu obrony narodowej, obejmujący swoim działaniem użytkowników z sił zbrojnych. Informacje o jego powołaniu zostały opublikowane za pośrednictwem resortowych sieci informatycznych – jawnej i niejawnej oraz rozpowszechnione korespondencyjnie. Zakres

[93] Wg stanu na dzień 29 września 2014 r.

działania Zespołu MIL-CERT.PL stanowią systemy informatyczne funkcjonujące w domenach „mon.gov.pl", „wp.mil.pl" oraz innych wykorzystywanych przez Siły Zbrojne RP. Misją Zespołu jest wytworzenie, utrzymywanie i wykorzystywanie zdolności do reagowania na incydenty bezpieczeństwa mające miejsce w tych domenach oraz prowadzenie działań zapobiegających takim incydentom. MIL-CERT.PL nie wykonywał innych działań i usług wykraczających poza określony powyżej formalny zakres, nie pełnił również roli krajowego punktu kontaktowego do spraw wymiany informacji z innymi zespołami CERT. Zespół nie uczestniczył w procesach: identyfikacji krytycznej infrastruktury informatycznej państwa, szacowania ryzyka oraz opracowywania planów ciągłości działania. MIL-CERT.PL nie otrzymał żadnych zadań na wypadek wystąpienia sytuacji kryzysowej związanej z funkcjonowaniem infrastruktury teleinformatycznej państwa. Zespół wykorzystuje opracowaną w resorcie obrony narodowej klasyfikację incydentów pozwalającą na ich identyfikację oraz przyporządkowanie adekwatnych procedur działania. W latach 2012–2014[94], MIL-CERT.PL obsłużył 11 174 incydenty, z których najpoważniejszy dotyczył poczty elektronicznej w systemie INTER-MON. Obecnie Zespół posiada 21 etatów. Koszty związane z zakupem, wdrożeniem i utrzymaniem systemów bezpieczeństwa w Zespole, w latach 2012–2014, wyniosły około 15,6 mln zł. Zespół MIL-CERT.PL utrzymuje kontakty z innymi zespołami CERT w kraju wykorzystując również, w wymagających tego przypadkach, komunikację szyfrowaną. Zespół dysponuje danymi kontaktowymi około 900 administratorów systemów teleinformatycznych w resorcie obrony narodowej.

W ocenie NIK, największym problemem polskiego systemu reagowania na incydenty komputerowe jest brak narodowego zespołu CERT, zarządzającego obsługą incydentów na terenie całej krajowej sieci i infrastruktury teleinformatycznej, dokonującego rozstrzygnięć w przypadkach wątpliwości co do kompetencji i zakresów działania poszczególnych zespołów krajowych, koordynującego ich aktywność w skomplikowanych przypadkach, wymagających zaangażowania dużych zasobów lub powiązania prowadzonych początkowo równolegle działań. Brakuje zespołu pełniącego rolę krajowego punktu kontaktowego, będącego z jednej strony miejscem międzynarodowej wymiany informacyjnej z zespołami z innych państw, a z drugiej przekazującego ważne sygnały i ustalenia do właściwych organów państwowych. Podstawowym wymogiem dla stworzenia takiego zespołu jest jego formalne wskazanie i opisanie w krajowym dokumencie strategicznym dotyczącym ochrony cyberprzestrzeni. Jego powstanie powinno zostać publicznie ogłoszone oraz zgłoszone do organizacji międzynarodowych. Obecna sytuacja, w której część zadań zespołu narodowego jest wykonywana na zasadach dobrowolnego zastępstwa przez CERT Polska, z jednej strony zabezpiecza przed skutkami istotnej luki w systemie reagowania na incydenty, ale z drugiej utwierdza ułomne, prowizoryczne rozwiązanie, niepozwalające np. wykorzystać w pełni współpracy z organizacjami międzynarodowymi, której nawiązanie wymaga formalnego potwierdzenia przez administrację rządową odpowiedniego statusu zespołu. **W ocenie NIK, zapisy „Polityki" wprowadziły w tym zakresie tylko dodatkowy chaos informacyjny wskazując, że CERT.GOV.PL „pełni rolę głównego zespołu CERT w obszarze administracji rządowej i obszarze cywilnym". Powyższe sformułowanie, wpisujące się w nieprecyzyjny język całej „Polityki", było dla części jej czytelników równoznaczne ze wskazaniem Zespołu z ABW, jako CERTu narodowego. Wyniki kontroli wykazały natomiast, że w chwili obecnej w Polsce nie ma CERTu narodowego, a rola taka nie została w ogóle zdefiniowana w polskim systemie prawnym**.

94 Wg stanu na dzień 22 sierpnia 2014 r.

Analiza przyjętych w Polsce rozwiązań z zakresu reagowania na incydenty komputerowe oraz działalności kontrolowanych zespołów CERT wykazała również problemy systemowe wpływające negatywnie na ich funkcjonowanie, dotyczące:

- **ograniczonych możliwości organizacyjnych w zakresie reagowania na incydenty** – wszystkie kontrolowane zespoły pracowały jedynie w dni robocze, w standardowych godzinach pracy (np. od 7:30 do 15:30). Tylko Zespół CERT.GOV.PL przygotowany jest, na wypadek sytuacji kryzysowej, do utrzymania dostępności swoich usług w trybie ciągłym – 24 godziny przez 7 dni w tygodniu;
- **braku jednolitej klasyfikacji incydentów** pozwalającej na porównywanie i korelowanie rejestrów prowadzonych przez poszczególne zespoły oraz przypisanych do nich ujednoliconych procedur działania i reagowania – jednoznaczność klasyfikacji oraz precyzyjne oznaczanie czasu dla poszczególnych informacji zapisywanych w rejestrach incydentów może mieć istotne znaczenie dla wykrywania ataków prowadzonych równolegle na wielu kierunkach oraz takich, w których podatność w jednym systemie pozwala uzyskać atakującym informacje umożliwiające atak na inny system;
- **ograniczeń organizacyjnych wynikających z umiejscowienia danego Zespołu**: Zespół MIL-CERT.PL działa jedynie w obszarze Sił Zbrojnych, CERT Polska jest przede wszystkim Zespołem wspomagającym konkretną działalność gospodarczą NASK, a CERT.GOV.PL usytuowany, w opinii wielu użytkowników cyberprzestrzeni, kontrowersyjnie w służbie specjalnej, nie posiada wystarczających zasobów oraz umocowania prawnego pozwalającego na egzekwowanie konkretnych działań od kierownictwa podmiotów objętych jego zakresem oddziaływania;
- **niewdrożenia zapisów pkt 4.2 i 4.3 „Polityki" dotyczących ustanowienia systemu łączności i wymiany informacji między różnymi rządowymi, cywilnymi i wojskowymi zespołami reagowania** – Minister Administracji i Cyfryzacji nie podejmował działań w celu wypracowania systemu łączności wspomagającego funkcjonowanie krajowego systemu reagowania na incydenty komputerowe w cyberprzestrzeni RP, nie dysponował wiedzą na temat kanałów wymiany informacji wykorzystywanych przez różne zespoły CERT oraz wskazywał wątpliwości interpretacyjne i brak zrozumienia zadań wynikających w tym zakresie z pkt 4.2 i 4.3 „Polityki".

W ocenie NIK, w Polsce jest zbyt mało państwowych zespołów reagowania na incydenty komputerowe, a ich organizacja nie jest postrzegana przez właścicieli systemów, jako dobra inwestycja w bezpieczeństwo. W trakcie kontroli nie stwierdzono m.in. powołania takich zespołów w Ministerstwach Spraw Wewnętrznych oraz Administracji i Cyfryzacji. Nie powołano go również w Policji, który to przykład jest szczególnie istotny przy porównaniu z realnie funkcjonującym systemem reagowania na incydenty w Siłach Zbrojnych – liczebność, siłowy charakter oraz ryzyko incydentów są dla obu formacji zbliżone. Należy jednocześnie podkreślić, że ustalona w trakcie kontroli wieloletnia praktyka funkcjonowania zespołów CERT wskazuje na silne powiązanie ich skuteczności z wiedzą, doświadczeniem, zaufaniem i osobistymi kontaktami każdego pracownika, których stopniowe zdobywanie jest niezbędnym wymogiem dla efektywnego podejmowania działań. Ten proces, z powodu swojej długotrwałości, silnie wpływa na możliwość modyfikacji istniejących i powoływania nowych zespołów reagowania – nie mogą one powstawać szybko, a budowa ich potencjału wymaga czasu. Stawia to szczególne wymagania przed procesem ewentualnych zmian w systemie ochrony cyberprzestrzeni RP. Należy zwrócić szczególną uwagę na utrzymanie obecnego poziomu ochrony i zaangażowanych w nią pracowników. Ewentualne

budowanie nowych struktur powinno uwzględniać uwarunkowania czasowe i organizacyjne związane z osiągnięciem niezbędnej sprawności oraz w maksymalnym zakresie utrzymać dotychczasowy potencjał.

Kontrola wykazała także, że nie został dotychczas zorganizowany system zbierania i rejestrowania informacji o incydentach występujących w cyberprzestrzeni. Nie wprowadzono prawnego obowiązku zgłaszania incydentów skierowanego do wszystkich najważniejszych użytkowników i administratorów cyberprzestrzeni[95], a jedyne istniejące w tym zakresie przepisy, zawarte w Prawie telekomunikacyjnym, były wadliwie sformułowane i całkowicie nieskuteczne.

W okresie od dnia wejścia w życie art. 175a ust. 1 Prawa telekomunikacyjnego[96], nakładającego obowiązek informowania o naruszeniach bezpieczeństwa lub integralności sieci lub usług, do dnia 30 czerwca 2014 r., przedsiębiorcy telekomunikacyjni przekazali Prezesowi UKE tylko 5 zgłoszeń dotyczących incydentów bezpieczeństwa związanych z cyberprzestrzenią. Zdecydowana większość zgłoszeń przekazywanych przez przedsiębiorców na podstawie ww. przepisu[97], dotyczyła awarii technicznych oraz zdarzeń losowych uniemożliwiających korzystanie z usług telefonii stacjonarnej. **Z ustaleń kontroli wynika natomiast, że w porównywalnym okresie[98], NASK była w posiadaniu informacji o około 40 milionach incydentów dotyczących sieci 9 największych krajowych przedsiębiorców telekomunikacyjnych.** Całkowita rozbieżność danych w tym zakresie wynikała m.in. z wadliwej konstrukcji art. 175a ust. 1 Prawa telekomunikacyjnego, który daje przedsiębiorcom telekomunikacyjnym swobodę w zakresie oceny istotności incydentów i zasadności ich zgłaszania do UKE. Szczegółowe dane liczbowe w tym obszarze zostały przedstawione na załączonych poniżej wykresach:

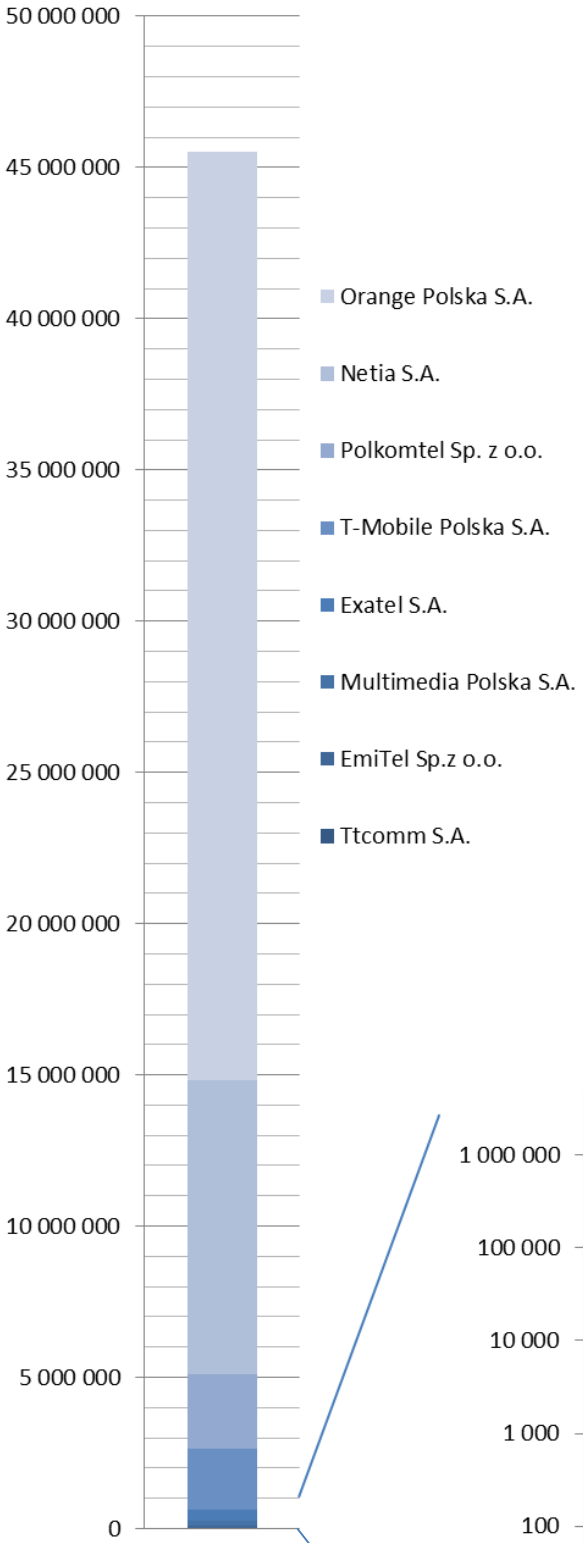
---

95 Zgodnie z opinią przedstawioną w opracowanej dla NIK przez Instytut Kościuszki ekspertyzie „Propozycja modelowych rozwiązań w zakresie budowania cyberbezpieczeństwa Polski", obowiązek raportowania o incydentach powinien dotyczyć przynajmniej operatorów infrastruktury krytycznej. Zobowiązania w tym zakresie powinny być zawarte m.in. w ustawie o zarządzaniu kryzysowym.

96 Tj., od 22 marca 2013 r.

97 W okresie od 22 marca 2013 r. do 30 czerwca 2014 r. przedsiębiorcy telekomunikacyjni poinformowali Prezesa UKE o 474 naruszeniach bezpieczeństwa lub integralności sieci i usług.

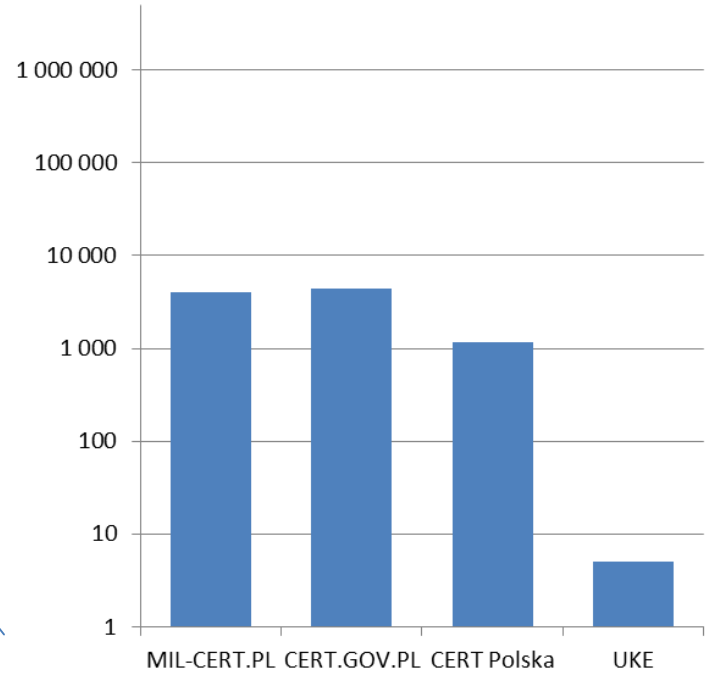
98 Informacje o incydentach dotyczą okresu 1 lipca 2013 r. – 30 czerwca 2014 r.



Na załączonych wykresach przedstawiono porównanie danych liczbowych za okres 12 miesięcy (1 lipca 2013 r. – 30 czerwca 2014 r.) dotyczących szacunkowej liczby incydentów w sieciach przedsiębiorców telekomunikacyjnych, zgłoszeń o incydentach przekazanych do UKE oraz incydentów obsłużonych przez poszczególne, objęte kontrolą państwowe zespoły CERT (zestawienia stanowią opracowanie własne NIK, sporządzone na podstawie danych liczbowych z poszczególnych jednostek objętych kontrolą).

Zsumowane na wykresie incydenty w sieciach przedsiębiorców telekomunikacyjnych dotyczyły adresów internetowych obsługiwanych przez te podmioty, zainfekowanych złośliwym oprogramowaniem, wykorzystywanych:

- **jako elementy składowe botnetów – 55%;**
- **do przeprowadzania ataków DDos – 43%;**
- **w innych celach (np. phishing) – 2%.**



Przedstawione dane wskazują, że administracja państwowa nie dysponuje nawet ogólną wiedzą na temat skali i rodzaju incydentów występujących w cyberprzestrzeni oraz m.in. ze względu na opisane wcześniej niewystarczające zasoby państwowych zespołów CERT i brak CERTu narodowego, nie ma możliwości koordynowania reakcji na incydenty.

Ustalono natomiast, że Minister Administracji i Cyfryzacji, odpowiadający zgodnie z pkt 4.2 „Polityki" za krajowy system reagowania na incydenty komputerowe nie realizował żadnych zadań w tym zakresie. Minister nie podjął działań w celu zorganizowania systemu wymiany informacji między MAiC a Zespołami CERT i innymi administratorami cyberprzestrzeni oraz w celu ustanowienia w Polsce narodowego Zespołu CERT. W Ministerstwie nie pozyskiwano i nie ewidencjonowano informacji na temat incydentów komputerowych występujących w cyberprzestrzeni. Nie realizowano i nie inicjowano działań wymienionych w pkt 3.6.2 oraz 3.6.5 „Polityki", dotyczących rozbudowy zespołów reagowania na incydenty komputerowe oraz ujednolicenia zakresów obowiązków tych zespołów i procedur reagowania. Minister Administracji i Cyfryzacji nie przeprowadzał analiz pozwalających na oszacowanie niezbędnych zasobów zespołów CERT – nie dysponował nawet wiedzą o strukturze, zasobach oraz o usługach świadczonych przez funkcjonujące państwowe zespoły CERT. Pomimo otrzymania od Prezesa UKE informacji na temat wadliwości przepisów dotyczących informowania przez przedsiębiorców telekomunikacyjnych o incydentach, w Ministerstwie nie przygotowano również projektu nowelizacji właściwych przepisów Prawa telekomunikacyjnego.

W ocenie NIK, ustalenia kontroli wskazują na konieczność podjęcia niezwłocznych działań w celu budowy krajowego systemu reagowania na incydenty komputerowe oraz wdrożenia realnych mechanizmów jego koordynacji. Świadczy o tym zarówno duża liczba incydentów i zagrożeń, jak i ich potencjalne, daleko idące skutki.

Ustanowienie i kontrola wymogów w zakresie bezpieczeństwa cyberprzestrzeni

W obowiązującym obecnie w Polsce porządku prawnym, wymogi dotyczące bezpieczeństwa informacji przetwarzanych w systemach teleinformatycznych zostały określone w § 20 rozporządzenia w sprawie Krajowych Ram Interoperacyjności. Przedmiotowa regulacja ma jednak ramowy charakter i ogranicza się tylko do systemów wykorzystywanych do realizacji zadań publicznych.

Stwierdzono natomiast, że kierownictwo podmiotów administracji państwowej, w tym w szczególności Minister Administracji i Cyfryzacji, nie podejmowało dotychczas działań w celu ustanowienia i wdrożenia kompleksowych wymogów bezpieczeństwa teleinformatycznego, dotyczących różnych grup użytkowników i administratorów cyberprzestrzeni, w tym podmiotów prywatnych. Jedynymi, zdefiniowanymi w trakcie kontroli wytycznymi bezpieczeństwa IT były:

- 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).

Przedmiotowe wytyczne zostały przygotowane w wyniku prac „Zespołu zadaniowego do spraw ochrony portali rządowych" i stanowiły odpowiedź na ataki ACTA, co potwierdza ustalenia niniejszej kontroli, że działania administracji państwowej związane z ochroną cyberprzestrzeni nie miały charakteru systemowego i stanowiły tylko doraźną reakcję na bieżące wydarzenia. Wytyczne miały bardzo ograniczony zakres oddziaływania (odnosiły się tylko do podmiotów administracji

państwowej), a ich wdrażanie nie było obowiązkowe – z okresowych analiz sporządzanych przez ABW, obejmujących ministerstwa i urzędy wojewódzkie wynika, że znaczna część zaleceń nie została uwzględniona i wdrożona przez kierownictwo tych podmiotów. Minister Administracji i Cyfryzacji, który pierwotnie współpracował z ABW w zakresie przygotowania i monitorowania stanu wdrożenia tych wytycznych, od momentu przekazania zadań związanych z cyberprzestrzenią do Departamentu Społeczeństwa Informacyjnego, nie podejmował dalszych działań w tym zakresie. Do końca kontroli, w MAiC nie rozpoczęto nawet prac związanych z przygotowaniem projektów standardów bezpieczeństwa oraz propozycji działań dla jednostek administracji rządowej, mających na celu ochronę systemów teleinformatycznych przed cyberatakami, pomimo iż ww. wytyczne, powinny były zostać przygotowane przez „Zespół zadaniowy do spraw bezpieczeństwa cyberprzestrzeni Rzeczypospolitej Polskiej" w terminie do dnia 13 grudnia 2014 r.

Brak systemowych działań ze strony Ministra Administracji i Cyfryzacji, tylko w niewielkim stopniu był rekompensowany oddolną aktywnością innych kontrolowanych podmiotów, dotyczącą tworzenia regulacji z zakresu bezpieczeństwa IT oraz upowszechniania w tym obszarze wzorów dobrych praktyk. Stwierdzonymi przykładami pozytywnych działań były:

- wdrażanie i monitorowanie przez kierownictwo MON szczegółowych wymogów dotyczących zarzadzania bezpieczeństwem sieci i systemów teleinformatycznych resortu obrony narodowej;
- zamieszczenie przez RCB w Załączniku nr 2 do Narodowego Programu Ochrony Infrastruktury Krytycznej ogólnych zasad i rekomendacji dotyczących ochrony teleinformatycznej obiektów infrastruktury krytycznej.

Kontrola wykazała także, że całkowicie martwe i niewykorzystywane w praktyce były przepisy art. 25 ust. 1 pkt 3 ustawy o informatyzacji, nakładające na ministrów i wojewodów obowiązki w zakresie przeprowadzania kontroli działania systemów teleinformatycznych używanych do realizacji zadań publicznych, obejmujących m.in. weryfikację wymogów bezpieczeństwa tych systemów wynikających z § 20 rozporządzenia w sprawie Krajowych Ram Interoperacyjności. Ustalono bowiem, że w całym okresie objętym badaniem:

- 14 z 16 wojewodów w ogóle nie realizowało obowiązków określonych w art. 25 ust. 1 pkt 3 lit. a ustawy o informatyzacji, dotyczących kontroli systemów teleinformatycznych wykorzystywanych przez jednostki samorządu terytorialnego i ich związki oraz w tworzonych lub prowadzonych przez te jednostki samorządowych osobach prawnych i innych samorządowych jednostkach organizacyjnych[99];
- Minister Administracji i Cyfryzacji oraz Minister Spraw Wewnętrznych nie planowali oraz nie przeprowadzali, wymaganych na podstawie art. 25 ust. 1 pkt 3 lit. b ww. ustawy, kontroli systemów teleinformatycznych wykorzystywanych przez podmioty podległe lub nadzorowane;
- Minister Administracji i Cyfryzacji nie planował i nie przeprowadzał kontroli wymaganych na podstawie art. 25 ust. 1 pkt 3 lit. c ww. ustawy, tj. we wszystkich pozostałych podmiotach publicznych wykorzystujących systemy teleinformatyczne;

Z wyjaśnień wojewodów oraz Kierownictwa MAiC i MSW wynikało, że głównymi powodami odstąpienia od realizacji zadań wymienionych w art. 25 ust. 1 pkt 3 ustawy o informatyzacji był brak

[99] Informacje i wyjaśnienia w ww. zakresie zostały uzyskane od wszystkich wojewodów, w trybie art. 29 ust. 1 pkt 2 lit. f ustawy o NIK, w ramach kontroli 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".

kadr posiadających certyfikaty uprawniające do prowadzenia kontroli systemów teleinformatycznych oraz ograniczenia budżetowe, nie pozwalające na zatrudnienie dodatkowych kontrolerów lub skierowanie pracowników na wymagane kursy i egzaminy. Wskazywano również, że w wyniku nowelizacji ustawy o informatyzacji z 2010 r.[100], która zniosła obowiązek rejestrowania systemów teleinformatycznych, nie dysponowano wiedzą na temat katalogu systemów wykorzystywanych do realizacji zadań publicznych. Przedmiotowe problemy zostały zgłoszone przez wojewodów, w lipcu 2012 r., Ministrowi Administracji i Cyfryzacji z prośbą o podjęcie stosownych działań oraz o wydanie jednolitych wytycznych precyzujących sposób realizacji obowiązków w zakresie kontroli systemów teleinformatycznych wykorzystywanych do realizacji zadań publicznych.

Stwierdzono natomiast, że Minister Administracji i Cyfryzacji, do czasu kontroli NIK, nie podjął żadnych działań organizacyjnych pozwalających na realizację zadań określonych w art. 25 ust. 1 pkt 3 ustawy o informatyzacji. W szczególności, nie opracował wytycznych dla innych podmiotów i nawet nie udzielił odpowiedzi na pytania skierowane w tym zakresie w imieniu innych wojewodów przez Wojewodę Podlaskiego. Nie wystąpił również do Ministra Finansów o przydzielenie dodatkowych środków finansowych na realizację zadań przewidzianych w ww. przepisach. Jedyne działania, rozpoczęte dopiero w trakcie kontroli NIK, dotyczyły przygotowania własnej komórki kontrolnej i polegały na skierowaniu 2 osób na szkolenia uprawniające do kontroli systemów teleinformatycznych oraz uruchomieniu procedury naboru dodatkowego pracownika z wymaganymi uprawnieniami.

W ocenie NIK, całkowite odstąpienie od przeprowadzania kontroli systemów teleinformatycznych, wymaganych na podstawie ustawy o informatyzacji, świadczy o tolerowaniu przez Kierownictwo MAiC i MSW sytuacji niestosowania przepisów i braku wykorzystania gotowych rozwiązań ustawowych do realizacji zadań związanych z ochroną cyberprzestrzeni państwa. NIK, nie podziela stanowiska przedstawionego w wyjaśnieniach, że brak formalnej ewidencji systemów wykorzystywanych do realizacji zadań publicznych całkowicie uniemożliwiał realizację obowiązków kontrolnych. Należy podkreślić, że kierownictwo badanych jednostek nie podjęło żadnych działań w celu wykorzystania powszechnie dostępnych baz danych i źródeł informacji na temat systemów teleinformatycznych, takich jak:

- informacje o systemach teleinformatycznych administracji publicznej dostępne na stronach internetowych Głównego Urzędu Statystycznego[101];
- przekazana do MAiC, baza danych państwowych systemów teleinformatycznych, przygotowana w formie elektronicznej przez Ministra Finansów po przeprowadzonym w 2013 r., zleconym audycie wewnętrznym bezpieczeństwa IT;
- informacje o systemach teleinformatycznych jednostek podległych i nadzorowanych przez poszczególnych Ministrów.

Ponadto, na podstawie art. 13 ustawy likwidującej Krajową Ewidencję Systemów Teleinformatycznych[102], minister właściwy ds. informatyzacji miał możliwość dalszego wykorzystywania zgromadzonych w niej danych, w celu ustalania stanu państwowych systemów teleinformatycznych.

[100] Ustawa z dnia 12 lutego 2010 r. o zmianie ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne oraz niektórych innych ustaw (Dz. U. Nr 40, poz. 230).

[101] http://bip.stat.gov.pl/dzialalnosc-statystyki-publicznej/polska-statystyka-publiczna/

[102] Ustawa z dnia 12 lutego 2010 r. o zmianie ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne oraz niektórych innych ustaw.

W ocenie NIK, jako całkowicie błędne należy również uznać stanowisko Ministra Administracji i Cyfryzacji, który wskazał w wyjaśnieniach, że w jego ocenie mechanizmy kontrolne ustanowione na podstawie art. 25 ustawy o informatyzacji (obejmujące m.in. weryfikację wymogów bezpieczeństwa systemów teleinformatycznych) nie są bezpośrednio związane z ochroną cyberprzestrzeni i stanowią tylko element ogólnie rozumianej kontroli zarządczej. Przedstawiona opinia świadczy o braku świadomości i nieprawidłowym zdefiniowaniu zadań Ministra związanych z bezpieczeństwem teleinformatycznym.

Rozwój narodowych planów kryzysowych związanych ze zdarzaniami występującymi w cyberprzestrzeni

W toku kontroli zidentyfikowano następujące procedury reagowania kryzysowego, wynikające z obowiązujących przepisów, które powinny określać schematy działania, pozwalające na skuteczną i adekwatną reakcję na zagrożenia związane z cyberprzestrzenią:

- 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 art. 176a ust. 1 i 2 Prawa telekomunikacyjnego.

Analiza, wymienionych powyżej procedur reagowania kryzysowego wykazała jednak, że nie zostały one dotychczas dostosowane do postępujących zmian technologicznych i wynikających z nich nowych niebezpieczeństw. Poszczególne, objęte kontrolą plany kryzysowe odnosiły się do zagrożeń konwencjonalnych i nie obejmowały reakcji na zdarzenia związane z bezpieczeństwem IT. W związku z powyższym, w ocenie NIK, w chwili obecnej brak jest kompleksowych procedur reagowania kryzysowego i utrzymania ciągłości działania podstawowych procesów ekonomicznych oraz funkcji państwa w sytuacji zagrożeń lub zakłócenia działania infrastruktury państwa spowodowanych zdarzeniami występującymi w cyberprzestrzeni, i tak:

- **w Krajowym Planie Zarządzania Kryzysowego** (zwanym dalej KPZK lub Planem), który został przyjęty przez Radę Ministrów 6 marca 2012 r. w ogóle nie uwzględniono zagrożeń związanych ze zdarzeniami występującymi w cyberprzestrzeni. 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[103]. W związku z powyższym w ww. dokumencie w ogóle **nie zawarto zadań i podmiotów odpowiedzialnych za zarządzanie zdarzeniami kryzysowymi występującymi w cyberprzestrzeni oraz całkowicie pominięto wiodącą rolę Ministra Administracji i Cyfryzacji w tym zakresie**. Propozycja uzupełniania KPZK o zdarzenia występujące w cyberprzestrzeni została zgłoszona przez Biuro Bezpieczeństwa Narodowego w trakcie międzyresortowej konferencji uzgodnieniowej poświęconej aktualizacji Planu, w styczniu 2013 r., natomiast wg stanu na dzień podpisania niniejszej informacji, przedmiotowe korekty nie zostały wprowadzone. Konieczność aktualizacji KPZK, pod kątem procedur reagowania kryzysowego związanych z ochroną cyberprzestrzeni, nie była zgłaszana

[103] Zapobieganie, przygotowanie, reagowanie, odbudowa.

przez Ministra Administracji i Cyfryzacji koordynującego działania w zakresie bezpieczeństwa teleinformatycznego, ani przez Ministra Spraw Wewnętrznych odpowiadającego za zarządzanie kryzysowe. Kierownictwo MAiC i MSW wyjaśniało, że niepodjęcie działań w tym zakresie wynikało m.in. z braku wiedzy i świadomości dotyczących konieczności aktualizacji KPZK o tematykę dotyczącą bezpieczeństwa IT. Dyrektor Departamentu Społeczeństwa Informacyjnego MAiC, odpowiadającego za ochronę cyberprzestrzeni wskazał także, że w jego opinii, tematyka planów kryzysowych związanych z zagrożeniami dla systemów teleinformatycznych, nie wchodzi w zakres zadań podległej mu komórki organizacyjnej.

W trakcie kontroli NIK, z inicjatywy RCB, została rozpoczęta, wymagana przepisami, okresowa aktualizacja KPZK, w ramach której przygotowano m.in. siatkę bezpieczeństwa dotyczącą zagrożeń w cyberprzestrzeni. Projekt ww. dokumentu, został przygotowany w sposób niepoprawny merytorycznie oraz z niezgodnie z uchwałą Rady Ministrów w sprawie przyjęcia „Polityki", ponieważ pominięto w nim wiodącą rolę Ministra Administracji i Cyfryzacji w zakresie koordynacji działań związanych z ochroną cyberprzestrzeni – dla wszystkich faz zarządzania kryzysowego, jako podmiot wiodący wskazano ABW. Projekt aktualizacji KPZK był opiniowany przez MAiC, natomiast Minister Administracji i Cyfryzacji nie wniósł uwag odnoszących się do nieprawidłowego przygotowania tego dokumentu. Z udzielonych wyjaśnień wynika, że zaakceptowano przypisanie zadań Ministra Administracji i Cyfryzacji dotyczących ochrony cyberprzestrzeni ABW, ponieważ MAiC nie ma zasobów wymaganych do realnego podejmowania działań w tym obszarze.

Kontrola wykazała także, że procedury reagowania na zdarzenia występujące w cyberprzestrzeni nie zostały wdrożone w Urzędzie obsługującym Ministra Administracji i Cyfryzacji. Od momentu utworzenia Ministerstwa do dnia zakończenia kontroli, nie został opracowany Plan Zarządzania Kryzysowego (PZK) MAiC. W projekcie ww. dokumentu, przygotowanym w lutym 2014 r., wymieniono zagrożenia związane z cyberprzestrzenią, natomiast nie wskazano dla tych zagrożeń, zagadnień wymienionych w art. 12 ust. 2 pkt 2 ustawy o zarządzaniu kryzysowym, tj. szczegółowych sposobów i środków reagowania oraz ograniczania i likwidacji ich skutków. Nie uwzględniono również wiodącej roli Ministra Administracji i Cyfryzacji w koordynacji działań związanych z bezpieczeństwem teleinformatycznym i nie wskazano w siatce bezpieczeństwa – Departamentu Społeczeństwa Informacyjnego odpowiadającego w Ministerstwie za realizację tych zadań. Na etapie wewnątrzresortowych uzgodnień projektu PZK MAiC, zarówno Członek Kierownictwa Ministerstwa odpowiadający za ochronę cyberprzestrzeni, jak i Kierownictwo Departamentu Społeczeństwa Informacyjnego nie zgłosili żadnych uwag dotyczących nieprawidłowego przygotowania tego dokumentu. Dopiero w trakcie kontroli NIK, rozpoczęto prace nad nową wersją Planu Zarządzania Kryzysowego Ministerstwa, uwzględniającą ww. zagadnienia;

- **do końca kontroli[104], dla żadnego z obiektów wymienionych w wykazie infrastruktury krytycznej nie został zatwierdzony, wymagany na podstawie art. 6 ust. 5 ustawy o zarządzaniu kryzysowym – plan ochrony infrastruktury krytycznej.** Powyższe wynikało m.in. z nieprecyzyjnego brzmienia §§ 3 i 4 rozporządzenia Rady Ministrów w sprawie planów ochrony infrastruktury krytycznej, w których wskazano termin sporządzenia planów[105] oraz

[104] Wg stanu na dzień 21 października 2014 r.

[105] 9 miesięcy od daty otrzymania od Dyrektora RCB informacji o ujęciu danego obiektu w wykazie infrastruktury krytycznej.

terminy ich uzgodnienia przez poszczególne podmioty, natomiast w żaden sposób nie określono ram czasowych na korektę nieprawidłowo przygotowanych planów oraz łącznego, nieprzekraczalnego terminu na zatwierdzenie tych dokumentów. Powyższe skutkowało możliwością praktycznie nieograniczonego czasowo opóźniania przyjęcia planów ochrony dla poszczególnych obiektów infrastruktury krytycznej.

Ustalono, że objęte kontrolą organy administracji rządowej, w tym w szczególności Dyrektor RCB oraz Minister Administracji i Cyfryzacji, nie podjęły rzetelnych działań w celu zapewnienia wysokiej jakości planów ochrony infrastruktury krytycznej i należytego uwzględnienia w tych dokumentach tematyki ochrony cyberprzestrzeni. Poza ogólnymi rekomendacjami zawartymi w Załączniku nr 2 do Narodowego Programu Ochrony Infrastruktury Krytycznej, nie wydano żadnych wytycznych dotyczących bezpieczeństwa systemów teleinformatycznych, które mogłyby zostać wykorzystane przez operatorów infrastruktury krytycznej w celu opracowania planów ochrony – pozostawiono w tym zakresie dowolność podmiotom zarządzającym tymi obiektami i uzależniono ich ewentualne działania od indywidulanej świadomości ich kierownictwa. W RCB oraz w skontrolowanych Ministerstwach nie wypracowano również kryteriów i metodyki oceny kompletności oraz merytorycznej poprawności planów ochrony infrastruktury krytycznej w zakresie bezpieczeństwa teleinformatycznego. Uzgadnianie ww. dokumentów polegało w znacznym stopniu na formalnym sprawdzeniu ich kompletności pod kątem przepisów rozporządzenia[106] i nie zapewniało realnej wiedzy na temat adekwatności wdrożonych zabezpieczeń i przyjętych procedur działania w sytuacji zagrożeń lub zakłócenia działania infrastruktury krytycznej spowodowanych zdarzeniami występującymi w cyberprzestrzeni. **W związku z powyższym, w ocenie NIK, istnieje ryzyko, że opracowane plany ochrony infrastruktury krytycznej, tylko w niewielkim stopniu będą mogły być wykorzystywane w ramach realizacji zadań związanych z ochroną cyberprzestrzeni**.

Należy również podkreślić, że Dyrektor RCB, który jest uprawniony do zatwierdzania planów ochrony oraz Minister Administracji i Cyfryzacji odpowiadający za koordynację działań w zakresie ochrony cyberprzestrzeni, nie dysponowali wiedzą na temat liczby, nazw i rodzaju systemów teleinformatycznych wchodzących w skład krajowej infrastruktury krytycznej[107]. Powyższe wynikało z faktu, że obowiązujące obecnie kryteria konstruowania wykazu infrastruktury krytycznej nie pozwalają na identyfikację poszczególnych systemów teleinformatycznych wchodzących w skład krytycznej infrastruktury państwa. Ustalono natomiast, że Minister Administracji i Cyfryzacji oraz kierownictwo innych instytucji państwowych nie zgłaszali do RCB żadnych uwag lub propozycji mających na celu wykorzystanie danych zbieranych w związku z tworzeniem wykazu infrastruktury krytycznej oraz ewentualnej modyfikacji kryteriów konstruowania tego wykazu. **Działania związane z bezpieczeństwem IT były zatem prowadzone bez fundamentalnej wiedzy, jakie są krytyczne państwowe zasoby teleinformatyczne, co świadczy o całkowitym braku spójności oraz komplementarności**

[106] Rozporządzenie Rady Ministrów w sprawie planów ochrony infrastruktury krytycznej.

[107] Obecnie obowiązujący jednolity wykaz obiektów, instalacji, urządzeń i usług wchodzących w skład infrastruktury krytycznej, został sporządzony i podpisany przez Dyrektora RCB 14 lipca 2014 r. Zawiera on 689 pozycji podzielonych na 11 systemów infrastruktury krytycznej. Systemy teleinformatyczne wchodzące w skład krajowej infrastruktury krytycznej zawarte są w szczególności w pozycjach: „Systemy łączności", „Systemy sieci teleinformatycznych" oraz „Systemy zapewniające ciągłość działania administracji publicznej", natomiast niewskazane wprost, występują one także w pozostałych systemach jako oddzielne obiekty, lub jako cześć składowa poszczególnych obiektów, instalacji, urządzeń i usług wchodzących w skład infrastruktury krytycznej.

procesów zarządzania kryzysowego i ochrony cyberprzestrzeni. Dopiero w trakcie kontroli NIK, MAiC i RCB rozpoczęły współpracę dotyczącą m.in. przeglądu kryteriów pozwalających na wyodrębnianie obiektów infrastruktury krytycznej pod kątem ich wykorzystania dla zapewnienia bezpieczeństwa cyberprzestrzeni RP. Podjęte w tym zakresie działania wynikały m.in. z ustaleń niniejszej kontroli wskazujących na nieuwzględnienie w wykazie infrastruktury krytycznej, w ramach „systemu sieci teleinformatycznych", za który odpowiada Minister Administracji i Cyfryzacji – obiektów kluczowych dla funkcjonowania Internetu w Polsce;

- **w wyniku badania 9 planów działań w sytuacjach szczególnych zagrożeń sporządzonych i przekazanych do UKE przez największych przedsiębiorców telekomunikacyjnych**[108] **ustalono, że w ww. dokumentach w ogóle nie wskazywano zagrożeń związanych ze zdarzeniami występującymi w cyberprzestrzeni (4 plany) lub wskazywano takie zagrożenia, ale nie zawarto adekwatnych do nich zabezpieczeń infrastruktury telekomunikacyjnej, procedur reagowania oraz struktur organizacyjnych przedsiębiorcy obowiązujących w przypadku wystąpienia zagrożeń związanych ze zdarzeniami występującymi w cyberprzestrzeni (4 plany)**[109]. Ponadto, jeden z przedsiębiorców wskazał, że ataki cybernetyczne nie stanowią zagrożenia dla jego infrastruktury, ponieważ jego zdaniem została ona fizycznie odseparowana od innych sieci i Internetu. Analizy zagrożeń sporządzane przez przedsiębiorców telekomunikacyjnych odnosiły się do konwencjonalnych niebezpieczeństw pochodzenia naturalnego (powodzie, pożary, śnieżyce, silne wiatry), katastrof technologicznych (skażenia przemysłowe i promieniotwórcze), katastrof komunikacyjnych (drogowe, budowlane), napadów, włamań oraz aktów terroru z wykorzystaniem przemocy fizycznej. Adekwatnie do tych zagrożeń, w planach działań opisywano tradycyjne, fizyczne zabezpieczenia infrastruktury telekomunikacyjnej oraz standardowe procedury reagowania nie odnoszące się bezpośrednio do bezpieczeństwa teleinformatycznego.

  Kierownictwo objętych kontrolą podmiotów, uczestniczących w uzgodnieniach planów działań przedsiębiorców telekomunikacyjnych, nie podejmowało działań w celu podniesienia jakości tych dokumentów. W szczególności, Szef Agencji Bezpieczeństwa Wewnętrznego i Minister Spraw Wewnętrznych, którzy powinni przekazywać przedsiębiorcom telekomunikacyjnym informacje służące identyfikacji ryzyk dla ich działalności[110], w pełni świadomie, nie wskazywali im żadnych zagrożeń związanych ze zdarzeniami występującymi w cyberprzestrzeni, co wyjaśniano brakiem obowiązków prawnych w tym zakresie. Powyższe, w ocenie NIK, świadczy o postrzeganiu ww. planów działania, wyłącznie jako formalny obowiązek wynikający z Prawa telekomunikacyjnego, a nie jako realne narzędzia możliwe do wykorzystania w sytuacjach zagrożenia przedsiębiorców telekomunikacyjnych, zarządzających kluczową infrastrukturą państwa.

---

[108] Badaniem objęto wszystkie plany ogólne sporządzone przez największych ogólnopolskich przedsiębiorców telekomunikacyjnych, wymienionych w części V załącznika do rozporządzenia Rady Ministrów z dnia 4 października 2010 r. w sprawie wykazu przedsiębiorców o szczególnym znaczeniu gospodarczo-obronnym (Dz. U. z 2014 r., poz. 303 ze zm.).

[109] Tj. elementów wymienionych w § 5 pkt 11 i 12 Rozporządzenie Rady Ministrów w sprawie planu działań przedsiębiorcy telekomunikacyjnego w sytuacjach szczególnych zagrożeń.

[110] Przedmiotowy obowiązek wynika z § 4 ust. 3 Rozporządzenia Rady Ministrów w sprawie planu działań przedsiębiorcy telekomunikacyjnego w sytuacjach szczególnych zagrożeń.

Organizacja ćwiczeń i testów systemu bezpieczeństwa cyberprzestrzeni RP

W pkt. 3.6.4 „Polityki" podkreślono konieczność prowadzenia okresowych ćwiczeń i testów systemu bezpieczeństwa cyberprzestrzeni RP. Wskazano również, że „wyniki ćwiczeń będą służyć ocenie aktualnej odporności cyberprzestrzeni na ataki, natomiast wnioski stanowić będą podstawę do przygotowania zaleceń do dalszych działań prewencyjnych". W trakcie kontroli sprawdzono, w jakim zakresie poziom bezpieczeństwa cyberprzestrzeni jest faktycznie weryfikowany poprzez prowadzenie ćwiczeń i testów.

Ćwiczenia pozwalają dokonać, w warunkach zbliżonych do rzeczywistych, weryfikacji założonych sposobów zapobiegania i minimalizowania skutków różnorodnych incydentów oraz sprawdzić skuteczność metod współpracy i kanałów wymiany informacji dedykowanych dla sytuacji nadzwyczajnych. Mogą być również miejscem spotkań osób zaangażowanych w różnych instytucjach i firmach w zapewnienie bezpieczeństwa. Istotnym jest sposób wykorzystania pozytywnych i negatywnych efektów prowadzonych ćwiczeń i testów pozwalający na doskonalenie procedur i metod ochrony.

W kontrolowanym okresie, podmioty państwowe nie były organizatorami żadnych ćwiczeń dotyczących bezpieczeństwa cyberprzestrzeni. W ograniczonym zakresie, problematyka bezpieczeństwa teleinformatycznego była uwzględniona w wewnętrznych ćwiczeniach dotyczących systemów łączności i dowodzenia organizowanych przez jednostki resortu obrony narodowej. Spośród kontrolowanych jednostek, największą aktywnością w zakresie uczestnictwa w ćwiczeniach wykazały się zespoły CERT, biorące udział (również z sukcesami) w tego typu wydarzeniach organizowanych przez podmioty zagraniczne i polskie instytucje prywatne (np. organizacje pozarządowe). Analizując ich wyniki należy jednak stwierdzić, że poza podwyższeniem kompetencji i specjalistycznej wiedzy pracowników oraz nawiązaniem kontaktów osobistych, kontrolowane jednostki nie wskazały, na wynikające z udziału w ćwiczeniach, inne korzyści np. organizacyjne, legislacyjne lub związane z definiowaniem dobrych praktyk. W ocenie NIK, jest to sytuacja nieprawidłowa, wskazująca na niewystarczające wykorzystywanie i upowszechnienie wyników ćwiczeń lub brak realnego zainteresowania nimi przez uczestników oraz inne podmioty związane z budowaniem systemu bezpieczeństwa cyberprzestrzeni w Polsce. Przykładowo w raportach z przeprowadzenia ćwiczeń Cyber-EXE Polska 2012 i 2013, organizowanych przez podmioty prywatne, zapisano następujące, istotne w opinii Izby i godne wdrożenia rekomendacje:

- istnieje potrzeba stworzenia standardowej procedury operacyjnej dotyczącej współpracy w obsłudze ataku z cyberprzestrzeni, powinna ona zawierać elementy (…) odnoszące się do współpracy pomiędzy podmiotami administracji publicznej i podmiotami sektora prywatnego;
- procedury zarządzania kryzysowego należy uzupełnić o procedury na wypadek ataku z cyberprzestrzeni;
- konieczne jest upowszechnienie wiedzy o obszarach działania zespołów CERT funkcjonujących w Polsce;
- należy powołać do życia forum wymiany doświadczeń dla operatorów infrastruktury krytycznej w obszarze ochrony teleinformatycznej;
- zdobywanie aktualnej wiedzy na temat wszelkich aspektów specyfiki cyberataków może mieć kluczowe znaczenie dla skutecznej obrony przed nimi, dlatego personel odpowiedzialny

za te zadania powinien mieć pełen dostęp do wiedzy oraz szkoleń w tym zakresie. Szkolenia powinny dotyczyć nie tylko osób bezpośrednio odpowiedzialnych za bezpieczeństwo teleinformatyczne, ale również wszystkich pracowników, których nieprawidłowe działanie może istotnie wpłynąć na poziom bezpieczeństwa (...).

Jednym z najbardziej skutecznych sposobów weryfikacji poziomu ochrony w odniesieniu do systemów teleinformatycznych jest prowadzenie testów bezpieczeństwa. Spośród kontrolowanych jednostek, testy wykonywane były przez NASK, ABW oraz jednostki resortu obrony narodowej[111]. Porównując łączną liczbę 25 testów przeprowadzonych przez te podmioty w okresie objętym kontrolą, do liczby ponad 500 systemów informatycznych eksploatowanych w tym samym okresie w polskiej administracji publicznej[112] należy stwierdzić, że ten sposób weryfikacji poziomu bezpieczeństwa jest stosowany w bardzo ograniczonym zakresie. Mała liczba przeprowadzanych testów, wynikała ze wskazanych już wcześniej ograniczeń w funkcjonowaniu państwowych zespołów reagowania na incydenty komputerowe, tj.: niewystarczających zasobów CERT.GOV.PL., uwarunkowań działalności gospodarczej NASK oraz w przypadku resortu obrony narodowej – weryfikacji jedynie systemów Sił Zbrojnych.

Znacznie większy był zakres testów dotyczących bezpieczeństwa witryn internetowych instytucji państwowych. W kontrolowanym okresie, ABW przeprowadziła ponad 130 tego rodzaju testów. Były one związane przede wszystkim z weryfikacją „Wytycznych Ministra Administracji i Cyfryzacji w zakresie ochrony portali informacyjnych administracji publicznej" opracowanych w wyniku incydentów związanych z protestami ACTA. NIK nie neguje zasadności przeprowadzania i użyteczności tego rodzaju testów. **Należy jednak wskazać, że duża dysproporcja w liczbie testów witryn i systemów teleinformatycznych, świadczy o wybiórczym postrzeganiu kwestii bezpieczeństwa cyberprzestrzeni**. Potwierdza ona również ocenę NIK, że działania związane z ochroną cyberprzestrzeni RP nie miały charakteru systemowego i polegały głównie na doraźnym reagowaniu na bieżące wydarzenia, takie jak protesty ACTA.

Kontrola wykazała, że Minister Administracji i Cyfryzacji, odpowiadający za realizację „Polityki", nie podejmował żadnych działań w celu opracowania założeń oraz wdrożenia systemu ćwiczeń bezpieczeństwa cyberprzestrzeni RP. W całym okresie objętym kontrolą, pracownicy Ministerstwa, dwukrotnie uczestniczyli w ćwiczeniach (z tego tylko jeden raz w formie aktywnego uczestnika) i poza tymi przypadkami nie otrzymywali nawet zaproszeń do udziału w tego rodzaju wydarzeniach. Świadczy to o marginalnej roli Ministra Administracji i Cyfryzacji w obszarze bezpieczeństwa cyberprzestrzeni, który nie był dotychczas postrzegany jako ważny partner, przez podmioty prywatne i organizacje międzynarodowe będące organizatorami ćwiczeń. W MAiC nie wypracowano także założeń określających pożądany model testów penetracyjnych, mających na celu weryfikację prawidłowości rozwiązań w zakresie bezpieczeństwa teleinformatycznego. Ministerstwo nie dysponowało wiedzą na temat skali testów penetracyjnych prowadzonych w jednostkach administracji państwowej przez rządowe Zespoły CERT oraz przez podmioty komercyjne.

[111] Poza kontrolowanymi jednostkami testy bezpieczeństwa systemów administracji publicznej były również prowadzone przez podmioty prywatne.

[112] Dane liczbowe o systemach informatycznych administracji publicznej uzyskano ze stron internetowych GUS.

System wczesnego ostrzegania przed zagrożeniami w sieci Internet

W trakcie kontroli, jako system wczesnego ostrzegania przed zagrożeniami w sieci Internet wykorzystywany był, wdrażany od 2005 r. przez ABW wraz z Zespołem CERT Polska, ARAKIS-GOV[113]. Jego architektura oparta została na rozproszonych sensorach instalowanych w wybranych instytucjach, w punktach styku ich wewnętrznej sieci komputerowej z Internetem. Centralna część systemu dokonuje korelacji informacji o zdarzeniach otrzymywanych z poszczególnych sensorów, określa ich związki czasowe, poszukuje anomalii (wskazujących na potencjalne zagrożenia) i prezentuje wyniki tych analiz w przystępnej formie. Wyniki pracy systemu, po analizie przez specjalistów ABW, pozwalają na wczesne wykrywanie prób nieautoryzowanego logowania oraz prób badania sieci przed planowanym atakiem lub pozyskiwania danych. Posługując się systemem ARAKIS.GOV można identyfikować znane i stosowane po raz pierwszy metody ataków, określać ich skalę oraz oceniać sprawność stosowanych środków zabezpieczających. **W trakcie kontroli, system posiadał około 70 sensorów zlokalizowanych w instytucjach ważnych z punktu widzenia funkcjonowania struktur państwowych**.

Ustalono, że zasięg oddziaływania systemu ARAKIS.GOV oraz pozyskiwanych za jego pomocą informacji miały ograniczony zakres, co wynikało w szczególności z:

- objęcia nadzorem systemu jedynie administracji państwowej – ograniczało to możliwość wykrycia anomalii dotyczących innych obszarów, np. infrastruktury krytycznej, bankowości, ochrony zdrowia lub telekomunikacji;
- możliwości technicznych infrastruktury NASK, pozwalających na obsługę maksymalnej liczby 100 sensorów, co stanowiło niewielki procent istotnych użytkowników i administratorów cyberprzestrzeni;
- finansowania sprzętu wchodzącego w skład systemu w całości z ograniczonego budżetu ABW (był on następnie wypożyczany współpracującym instytucjom);
- nieaktualnej i przestarzałej architektury systemu, co wynikało z postępującej w ciągu 10 lat jego wykorzystywania ewolucji zagrożeń i metod ich wykrywania połączonej z ograniczonymi możliwościami jego modernizacji;
- utrudnionego zarządzania rozproszoną na terenie całego kraju infrastrukturą;
- serwisowania systemu jedynie przez ABW – koszty serwisu były dodatkowo podwyższone poprzez znaczne wyeksploatowanie systemu, którego elementy w większości zakupiono w latach 2005–2007.

Postępujące techniczne „starzenie" się systemu, spowodowało konieczność rozpoczęcia prac nad jego nową wersją – ARAKIS 2.0. Dzięki zastosowaniu nowej architektury możliwa będzie rozbudowa tego narzędzia poprzez dołączanie kolejnych sensorów o rozszerzonych możliwościach oraz unowocześnionych algorytmów wykrywania anomalii. W trakcie kontroli, prace projektowe związane z ARAKIS 2.0 były już zakończone, uruchomiono prototyp tego systemu i rozpoczęto jego wdrażanie. Planowany termin zakończenia projektu to październik 2015 r.

Kontrola wykazała, że rozbudowa systemu wczesnego ostrzegania była jedynym realnie prowadzonym, sformalizowanym przedsięwzięciem mającym związek z wymienionymi w „Polityce"

[113] Odrębny system ostrzegania o zagrożeniach funkcjonuje w resorcie obrony narodowej.

działaniami na rzecz podnoszenia bezpieczeństwa teleinformatycznego państwa. Ten niewielki sukces w realizacji tego dokumentu wynikał z faktu, że prace projektowe dotyczące ARAKIS 2.0 rozpoczęto już w roku 2011, a więc na długo przed przyjęciem „Polityki". Znamiennym jest także, że modernizacja systemu wczesnego ostrzegania przebiegała bez praktycznego związku z „Polityką" – zapisany w pkt 3.6.3 tego dokumentu projekt szczegółowy dotyczący rozbudowy ARAKIS.GOV nie został nawet formalnie rozpoczęty, a Minister Administracji i Cyfryzacji odpowiadający za wdrażanie „Polityki" nie uczestniczył w realizacji tego przedsięwzięcia i nie dysponował żadną wiedzą na jego temat. **Należy także wskazać, że pomimo podjętych działań w celu rozbudowy i modernizacji ARAKIS.GOV, nie zostało wyeliminowane podstawowe ograniczenie tego systemu, dotyczące objęcia jego nadzorem jedynie administracji państwowej. Nie zostały natomiast podjęte żadne działania, mające na celu zaplanowanie budowy ogólnokrajowego systemu wczesnego ostrzegania, zapewniającego rzetelną wiedzę o zagrożeniach w sieci Internet, dotyczących krytycznej infrastruktury państwa**.

Szkolenia i działania edukacyjne

Większość kontrolowanych jednostek wskazywała na problemy z pozyskiwaniem wykwalifikowanych specjalistów z zakresu ochrony cyberprzestrzeni. Podkreślano, że utrzymujący się obecnie w obszarze teleinformatyki wysoki popyt na pracowników skutkuje wzrostem stawek wynagrodzeń funkcjonujących na rynku, zwłaszcza w sytuacji, gdy nie jest on ograniczony przez regulacje prawne. W efekcie wynagrodzenia informatyków w sferze komercyjnej znacznie przewyższają stawki pracowników sfery budżetowej, ograniczone utrzymywanym od 2006 r. zamrożeniem i brakiem waloryzacji płac. System wynagradzania stosowany w administracji państwowej nie pozwala także na zastosowanie odrębnych siatek płac dla pracowników posiadających szczególne umiejętności. Instytucje państwowe starają się zatem stosować inne niż ekonomiczne zachęty dla pracowników – możliwość uczestnictwa w szkoleniach, dostęp do ekskluzywnej wiedzy oraz udział w ćwiczeniach i współpracy międzynarodowej. Jest to jednak metoda ułomna, powodująca realnie wzrost fluktuacji kadr – pracownicy po kilku latach i uzyskaniu wiedzy, kwalifikacji i kontaktów na rynku, odchodzili do lepiej płatnej pracy w firmach prywatnych.

W trakcie kontroli nie stwierdzono funkcjonowania systemu szkoleń pozwalającego na uzyskiwanie i podnoszenie kwalifikacji pracowników w obszarze ochrony cyberprzestrzeni, w tym w szczególności pełnomocników do spraw bezpieczeństwa cyberprzestrzeni, w skład którego powinny wchodzić:

- katalog ról osób odpowiedzialnych za ochronę cyberprzestrzeni oraz użytkowników cyberprzestrzeni wraz z wymaganiami dotyczącymi ich wykształcenia i kwalifikacji;
- programy szkoleń przypisanych do poszczególnych ról;
- wymagania dotyczące podmiotów prowadzących szkolenia i częstotliwości szkoleń;
- wymagania dotyczące egzaminów i weryfikacji jakości szkoleń;
- ewidencja osób przeszkolonych.

Minister Administracji i Cyfryzacji nie podejmował działań w celu stworzenia takiego systemu. Nie opracował również żadnych wytycznych, ani zaleceń dotyczących szkoleń z zakresu bezpieczeństwa teleinformatycznego. Aktywność Ministra w tym obszarze ograniczyła się

do zorganizowania w 2014 r. trzech szkoleń[114] skierowanych przede wszystkim do pełnomocników do spraw bezpieczeństwa cyberprzestrzeni.

Spośród kontrolowanych jednostek, w ABW, MON i Policji były prowadzone wewnętrzne kursy i szkolenia specjalistyczne z zakresu różnych aspektów cyberbezpieczeństwa. Dotyczyły one przede wszystkim osób realizujących zadania związane z zagrożeniami w cyberprzestrzeni, w tym, ściganiem występujących w niej przestępstw. Na pozytywna ocenę zasługują, w szczególności, działania w zakresie edukacji podejmowane w resorcie obrony narodowej. W związku ze stworzeniem Narodowego Centrum Kryptologii i zidentyfikowaniem wynikających z tego potrzeb w zakresie pozyskania specjalistów, na Wydziale Cybernetyki Wojskowej Akademii Technicznej utworzono nowy kierunek studiów Kryptologia i Cyberbezpieczeństwo, którego zadaniem jest kształcenie specjalistów na potrzeby jednostek MON w tym NCK.

Uwagi NIK, dotyczyły natomiast NASK, w przypadku której stwierdzono, że pomimo pełnionej przez ten instytut szczególnej roli w zakresie zapewnienia cyberbezpieczeństwa na poziomie ogólnokrajowym, nie został w nim wprowadzony system wewnętrznych szkoleń z zakresu bezpieczeństwa IT dedykowany dla poszczególnych grup pracowników. W ocenie Izby, pomimo dysponowania przez niektórych pracowników NASK unikalnym poziomem wiedzy w obszarze bezpieczeństwa teleinformatycznego, brak powszechnych szkoleń, w istotny sposób zwiększył ryzyko wystąpienia incydentu bezpieczeństwa.

Kontrola wykazała również brak systemowego podejścia do działań edukacyjnych dotyczących zagrożeń występujących w cyberprzestrzeni. Stwierdzono w szczególności, że przepisy art. 175e ust. 1 Prawa telekomunikacyjnego, nie stanowiły podstawy rzetelnych i aktualnych informacji kierowanych do konsumentów na temat zagrożeń związanych z korzystaniem z Internetu oraz podstawowych, rekomendowanych środków ostrożności w tym zakresie. W okresie od wejścia w życie ww. przepisów, do końca kontroli[115], Prezes UKE opublikował tylko jeden poradnik zawierający ww. informacje, który nie podlegał aktualizacjom, a ponadto był trudno dostępny dla abonentów – jego odnalezienie wymagało otworzenia szeregu kolejnych zakładek na stronach internetowych Urzędu. W związku z powyższym, NIK zwróciła uwagę na niewystarczającą aktywność Prezesa UKE, który w obowiązującym obecnie porządku prawnym, jest jedynym organem państwowym, docierającym bezpośrednio do konsumentów z informacjami na temat zagrożeń związanych z korzystaniem z Internetu, ich potencjalnych skutków oraz środków ochrony. Innym stwierdzonym problemem było niedysponowanie przez UKE rzetelną wiedzą o incydentach występujących w sieciach przedsiębiorców telekomunikacyjnych, która to wiedza mogłaby być wykorzystywana na potrzebę przygotowywania komunikatów dla konsumentów (szczegółowo opisano na str. 57–58 informacji).

Pomimo braku systemowego podejścia do edukacji w zakresie cyberbezpieczeństwa i nieopracowania w tym zakresie przez MAiC wytycznych lub zaleceń, w trakcie kontroli zidentyfikowano przykłady różnorodnych dobrych praktyk, dotyczących działań edukacyjnych prowadzonych przez kontrolowane jednostki, i tak:

[114] Dwa szkolenia jednodniowe i jedno dwudniowe.

[115] Tj. od 22 marca 2013 r. do 25 lipca 2014 r.

NASK

- projekt Saferinternet.pl – którego celem jest zwiększanie społecznej świadomości na temat zagrożeń, jakie niosą ze sobą najnowsze techniki komunikacji;
- projekt Helpline.org.pl – w ramach którego udzielana jest pomoc młodym internautom, rodzicom i profesjonalistom w przypadkach zagrożeń związanych z korzystaniem z Internetu oraz telefonów komórkowych przez dzieci i młodzież;
- projekt Dyżurnet.pl – punkt kontaktowy, tzw. hotline, do którego można anonimowo zgłaszać przypadki występowania w Internecie treści zabronionych prawem, takich jak pornografia dziecięca, pedofilia, treści o charakterze rasistowskim i ksenofobicznym;
- SECURE – coroczna konferencja na temat bezpieczeństwa teleinformatycznego.

ABW

- serfujbezpiecznie.pl – witryna przeznaczona dla wszystkich użytkowników cyberprzestrzeni propagująca zasady bezpiecznego korzystania z Internetu;
- cykl bezpłatnych szkoleń dla administratorów systemów teleinformatycznych administracji publicznej;
- codzienny biuletyn Zespołu CERT.GOV.PL, zawierający syntetyczną informację o aktualnych incydentach i zagrożeniach.

RCB

- CIIP focus – opracowywany kwartalne 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;
- konferencja Ochrona Teleinformatyczna Infrastruktury Krytycznej – skierowana do operatorów infrastruktury krytycznej oraz podmiotów sektora elektroenergetycznego.

MON

- projekt profilaktyczny „Bezpieczeństwo użytkowników w sieci" – cykl szkoleń skierowanych do środowiska wojskowego realizowany przez Żandarmerię Wojskową.

Wspieranie badań i rozwoju w obszarze ochrony cyberprzestrzeni

W trakcie kontroli dokonano analizy działań podejmowanych przez Narodowe Centrum Badań i Rozwoju[116] (NCBiR) w zakresie wspierania i koordynowania projektów badawczo-rozwojowych dotyczących ochrony cyberprzestrzeni. Ustalono, że ww. problematyka jest uwzględniana w ramach organizowanych przez NCBiR konkursów na finansowanie z budżetu państwa projektów w ramach tak zwanych „Strategicznych programów badań naukowych i prac rozwojowych" – obecnie dotyczy to siedmiu strategicznych, interdyscyplinarnych kierunków w tym „bezpieczeństwa i obronności państwa". Działania NCBiR dotyczące tej tematyki są realizowane w porozumieniu z Ministrem Obrony Narodowej, Ministrem Spraw Wewnętrznych, Agencją Bezpieczeństwa Wewnętrznego oraz Policją.

[116] NIK nie przeprowadziła kontroli w Narodowym Centrum Badań i Rozwoju. Informacje i wyjaśnienia dotyczące realizacji projektów naukowo-badawczych związanych z ochroną cyberprzestrzeni zostały uzyskane w trybie art. 29 ust. 1 pkt 2 lit. f ustawy o NIK z Ministerstwa Nauki i Szkolnictwa Wyższego, Narodowego Centrum Badań i Rozwoju oraz od beneficjantów tych projektów – Akademii Górniczo-Hutniczej, Wojskowego Instytutu Łączności oraz Instytutu Łączności.

W okresie objętym kontrolą NCBiR współfinansowało 5 projektów związanych tematycznie z ochroną cyberprzestrzeni RP, z których cztery zostały już zakończone. Łączna wartość ich dofinansowania ze środków budżetu państwa wyniosła 17,3 mln zł. Analiza celów osiągniętych w ramach ww. projektów wskazała na ograniczony zakres ich praktycznych wdrożeń i aplikacji. Projekty, zgodnie z planami, zakończono na etapie weryfikacji prototypów, ramowej architektury lub opracowaniu wymagań i koncepcji dla kolejnych etapów. Jedynie jeden z nich osiągnął poziom eksploatacji próbnej, jednak prowadzono ją w prywatnej spółce. Zdaniem NIK, należy zatem wskazać, że realizowana z wykorzystaniem państwowych dotacji działalność naukowo-badawcza ograniczała się praktycznie do rozwoju potencjału jej wykonawców. Prowadzone projekty nie były ze sobą powiązane, ich cele nie wpisywały się w jednolitą strategię. Brakowało również realnych potrzeb dla ich praktycznego zastosowania w celu podnoszenia poziomu bezpieczeństwa teleinformatycznego państwa.

Kontrolowane jednostki w różnym zakresie brały udział w realizacji badań i rozwoju w zakresie ochrony cyberprzestrzeni:

- MAiC – nie składało propozycji tematów naukowo-badawczych dotyczących ochrony cyberprzestrzeni RP i w ograniczonym zakresie współuczestniczyło tylko w jednym z projektów koordynowanych przez NCBiR;
- NASK – poza udziałem w projektach koordynowanych przez NCBiR, realizowała 7 projektów, finansowanych ze środków własnych oraz pochodzących z programów międzynarodowych;
- MON – poza udziałem w programach koordynowanych przez NCBiR, realizowano 10 projektów finansowanych w ramach programów badawczych resortu. Prowadzone je we współpracy z uczelniami i instytutami wojskowymi oraz cywilnymi. W związku z utworzeniem NCK zaproponowano utworzenie w NCBiR odrębnego programu strategicznego badań naukowych i prac rozwojowych, dotyczącego kryptologii i cyberbezpieczeństwa, zakładając zrealizowanie 33 projektów w latach 2015–2025;
- Policja – Wyższa Szkoła Policji w Szczytnie prowadziła samodzielnie lub we współpracy z podmiotami prywatnymi prace naukowo-badawcze związane z ochroną przed cyberprzestępczością i cyberterroryzmem.

Pozostałe jednostki: RCB, MSW oraz UKE nie uczestniczyły w realizacji i wdrażaniu projektów naukowo-badawczych związanych z ochroną cyberprzestrzeni.

4 INFORMACJE DODATKOWE

4.1 Organizacja i metodyka kontroli

W związku z brakiem jednolitych regulacji prawnych, określających w sposób spójny i precyzyjny ramy krajowego systemu ochrony cyberprzestrzeni, **przygotowanie kontroli obejmowało przede wszystkim zdefiniowanie zbioru dobrych praktyk**, stanowiącego wyznacznik kontrolowanej działalności. W ramach poszukiwania dobrych praktyk przeprowadzono w szczególności następujące analizy:

- wystąpiono o przekazanie dokumentacji oraz przeprowadzono konsultacje z przedstawicielami następujących instytucji państwowych i międzynarodowych zaangażowanych w proces ochrony cyberprzestrzeni: ENISA, MAiC, ABW, MF, KPRM, RCB, MSW, MON, NCBiR, Rządowe Centrum Legislacji, Biuro Bezpieczeństwa Narodowego, Ministerstwo Nauki i Szkolnictwa Wyższego, Ministerstwo Infrastruktury i Rozwoju;
- zwrócono się do najwyższych organów kontrolnych z kilkunastu wybranych państw z prośbą o przekazanie doświadczeń i dokumentacji z przeprowadzonych dotychczas kontroli związanych z cyberbezpieczeństwem (m.in. USA, Wielka Brytania, Niemcy, Francja, Hiszpania, Łotwa, Szwajcaria);
- przeprowadzono szereg konsultacji z niezależnymi ekspertami i przedstawicielami nauki, m.in. z Fundacją Bezpieczna Cyberprzestrzeń oraz Instytutem Kościuszki;
- podjęto próbę kontaktu z funkcjonującymi w Polsce państwowymi i prywatnymi zespołami CERT, przedstawicielami biznesu zaangażowanego w bezpieczeństwo IT oraz uczestnikami ABUSE Forum[117];
- przeprowadzono panel ekspertów z udziałem przedstawicieli instytucji państwowych oraz niezależnych ekspertów zajmujących się tematyką bezpieczeństwa teleinformatycznego.

Przeprowadzone działania, pomimo napotkanej w niektórych przypadkach niechęci do dialogu oraz trudności komunikacyjnych, pozwoliły na przygotowanie tematyki kontroli oraz określenie podstawowego katalogu zadań, które powinny być realizowane przez podmioty państwowe w związku z ochroną cyberprzestrzeni.

4.2 Postępowanie kontrolne i działania podjęte po zakończeniu kontroli

Przeprowadzona kontrola miała charakter krzyżowy, tzn. informacje i ustalenia uzyskane w jednej jednostce, były na bieżąco weryfikowane w innych podmiotach objętych badaniem. Ostatnim podmiotem, w którym zakończono czynności kontrolne było MAiC.

W wystąpieniach pokontrolnych, skierowanych do kierowników jednostek objętych kontrolą, Najwyższa Izba Kontroli sformułowała 20 wniosków pokontrolnych, związanych z bezpieczeństwem teleinformatycznym i budową krajowego systemu ochrony cyberprzestrzeni:

Do Ministra Administracji i Cyfryzacji o:

- przeprowadzenie, w trybie pilnym, kompleksowej analizy zadań Ministra 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;

[117] Abuse Forum to nieformalna organizacja zrzeszająca przedstawicieli różnych podmiotów działających na rzecz poprawy bezpieczeństwa teleinformatycznego w Polsce, m.in. operatorów telekomunikacyjnych, dostawców Internetu, banków i CERT-ów, służąca wymianie informacji i doświadczeń w zakresie prewencji i reagowania na zagrożenia występujące w cyberprzestrzeni.

- rzetelne oszacowanie zasobów (ludzkich, finansowych i rzeczowych) Ministerstwa oraz innych instytucji państwowych niezbędnych do budowy i skutecznego funkcjonowania krajowego systemu ochrony cyberprzestrzeni;
- 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;
- bezzwłoczne 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.

Do kierowników pozostałych jednostek objętych kontrolą, w szczególności o:

- podjęcie, w uzgodnieniu z Ministrem Administracji i Cyfryzacji, działań mających na celu zdefiniowanie roli i zadań kierowanych przez nich podmiotów, w ramach budowanego systemu ochrony cyberprzestrzeni RP[118];
- realizację zadań wynikających z „Polityki", dotyczących m.in. przeprowadzenia analizy ryzyka dla własnych zasobów teleinformatycznych[119] oraz oszacowania zasobów niezbędnych do realizacji zadań związanych z ochroną cyberprzestrzeni RP[120];
- wdrożenie efektywnych procedur dotyczących raportowania i ewidencjonowania incydentów bezpieczeństwa odnoszących się do wszystkich policyjnych sieci i systemów teleinformatycznych oraz podjęcie działań w celu utworzenia w Policji wewnętrznego zespołu reagowania na incydenty komputerowe[121];
- podjęcie, we współpracy z Ministrem Administracji i Cyfryzacji, działań mających na celu opracowanie projektu zmian legislacyjnych, pozwalających na praktyczne wykorzystanie przepisów Prawa telekomunikacyjnego w ramach realizacji zadań związanych z ochroną cyberprzestrzeni RP, w szczególności w zakresie uzyskiwania informacji o incydentach oraz tworzenia przez przedsiębiorców telekomunikacyjnych planów działania w sytuacjach kryzysowych związanych ze zdarzeniami występującymi w cyberprzestrzeni[122];
- przeprowadzenie analizy w zakresie możliwości zintensyfikowania działań informacyjnych UKE skierowanych do konsumentów w obszarze zagrożeń związanych z korzystaniem z Internetu oraz rekomendowanych środków ochronnych[123];
- podjęcie działań w celu realizacji obowiązków kontrolnych, wynikających z art. 25 ust. 1 pkt 3 lit. b ustawy o informatyzacji[124].

118 Minister Spraw Wewnętrznych, Minister Obrony Narodowej, Dyrektor RCB, Prezes UKE.
119 Minister Spraw Wewnętrznych.
120 Minister Spraw Wewnętrznych, Minister Obrony Narodowej, Prezes UKE, Komendant Główny Policji.
121 Komendant Główny Policji.
122 Prezes UKE.
123 Prezes UKE.
124 Minister Spraw Wewnętrznych.

Kierownicy siedmiu jednostek objętych kontrolą[125] nie skorzystali z prawa do zgłoszenia zastrzeżeń do wystąpienia i poinformowali NIK o sposobie wykorzystania uwag i wykonania wniosków pokontrolnych. Z udzielonych odpowiedzi wynika, że wg stanu na dzień 25 marca 2015 r., wszystkie wnioski pokontrolne skierowane do tych podmiotów (16 wniosków) znajdowały się w trakcie realizacji.

Zastrzeżenia do wystąpienia pokontrolnego zostały zgłoszone w dniu 12 lutego 2015 r. przez Ministra Administracji i Cyfryzacji. W zastrzeżeniach Minister zanegował w szczególności fakt, że jest on organem administracji rządowej odpowiadającym za koordynację działań związanych z ochroną cyberprzestrzeni RP oraz za utworzenie krajowego systemu reagowania na incydenty komputerowe. W związku z powyższym wskazał również na brak możliwości realizacji sformułowanych przez NIK wniosków pokontrolnych.

Uchwałą Nr 16/2015 Kolegium NIK z dnia 25 marca 2015 r. zastrzeżenia Ministra Administracji i Cyfryzacji zostały oddalone w całości.

[125] MSW, RCB, UKE, ABW, NASK, MON, KGP.

Wzory dobrych praktyk w zakresie ochrony cyberprzestrzeni

W związku z brakiem precyzyjnych i kompleksowych norm prawnych określających działania związane z ochroną cyberprzestrzeni państwa, kluczowe znaczenie ma wykorzystywanie **dobrych praktyk** wypracowanych przez instytucje posiadające w tym zakresie bogate doświadczenia. Wzorami takich dobrych praktyk wykorzystywanymi na etapie planowania kontroli były:

- Wytyczne ENISA dotyczące budowy i wdrażania narodowych strategii bezpieczeństwa cyberprzestrzeni[126];
- Wytyczne firmy Microsoft dotyczące budowania narodowych strategii bezpieczeństwa cyberprzestrzeni[127];
- Wytyczne ENISA dotyczące podstawowych wymogów dla narodowych/rządowych zespołów CERT[128];
- doświadczenia innych państw budujących krajowe systemy ochrony cyberprzestrzeni[129].

Zgodnie z wymienionymi powyżej wzorami dobrych praktyk tworzenie i wdrażanie narodowej strategii w zakresie ochrony cyberprzestrzeni powinno obejmować w szczególności następujące zadania i procesy:

1. **Określenie wizji, zakresu, celów i priorytetów narodowej strategii ochrony cyberprzestrzeni, tj.:**
   - zdefiniowanie głównych celów, które mają być osiągnięte w wyniku realizacji strategii w określonych ramach czasowych (z reguły 5–10 lat);
   - określenie zakresu oddziaływania strategii oraz jej adresatów;
   - opracowanie hierarchii celów szczegółowych strategii;
   - określenie „mapy drogowej" wdrożenia strategii (zadania, struktura zarządzania, konkretne plany działania dla poszczególnych obszarów, mierniki realizacji celów i zadań).
2. **Oszacowanie ryzyka na poziomie narodowym** – jest podstawą określenia celów i zakresu narodowej strategii ochrony cyberprzestrzeni oraz pozwala skoncentrować ograniczone krajowe zasoby na najpoważniejszych zagrożeniach. Szacowanie ryzyka powinno obejmować:
   - określenie jednolitej metodologii szacowania ryzyka;
   - określenie krytycznych sektorów z punktu widzenia funkcjonowania państwa i gospodarki;
   - identyfikację i szacowanie ryzyk;
   - określenie sposobu zarządzania poszczególnymi grupami ryzyk, tj. takich które będzie się ograniczać, akceptować i tych w stosunku, do których nie będą podejmowane żadne działania[130];

[126] European Network and Information Security Agency, "National Cyber Security Strategies, Practical Guide on Development and Execution", grudzień 2012 r. – tłumaczenie własne NIK.

[127] Cristin Flynn Goodwin, J. Paul Nicholas, "Developing a National Strategy for Cybersecurity, Foundations for Security, Growth, and Innovation", październik 2013 r. – tłumaczenie własne NIK.

[128] European Network and Information Security Agency, "Baseline Capabilities of National/Governmental CERTs, Updated Recommendations 2012", październik 2012 r. – tłumaczenie własne NIK.

[129] W ramach analizy przedkontrolnej NIK wystąpiła do najwyższych organów kontrolnych 12 państw z prośbą o przekazanie informacji na temat funkcjonujących w tych krajach rozwiązań systemowych w zakresie ochrony cyberprzestrzeni.

[130] Wytyczne ENISA i Microsoft kładą nacisk na świadome podejmowanie decyzji dotyczących reakcji na poszczególne grupy ryzyk.

- utworzenie narodowego rejestru ryzyk;
- ustanowienie procesu bieżącego aktualizowania wyników analizy ryzyka.

Zgodnie z wytycznymi ENiSA i Microsoft szacowanie ryzyka powinno być procesem ciągłym oraz obejmować jak najszerszy proces konsultacyjny. W szczególności, wymagany jest udział w ww. procesie podmiotów sektora komercyjnego i operatorów infrastruktury krytycznej, którzy mają największą wiedzę na temat specyfiki funkcjonowania poszczególnych sektorów gospodarki, potencjalnych zagrożeń i koniecznych działań zaradczych. Na podstawie przeprowadzonego szacowania ryzka możliwe jest określenie pożądanego poziomu zabezpieczeń poszczególnych elementów infrastruktury państwa.

3. **Analiza istniejących i funkcjonujących już w obszarze ochrony cyberprzestrzeni zasobów** (np. CERTy), **regulacji** (np. obowiązek informowania przez operatorów telekomunikacyjnych o incydentach), przypisanych **zadań i kompetencji poszczególnych podmiotów** – weryfikacja na ile funkcjonujące już rozwiązania są kompletne, a gdzie wymagają uzupełnienia.
4. **Identyfikacja i zaangażowanie uczestników systemu ochrony cyberprzestrzeni**. Zgodnie z wytycznymi ENiSA i Microsoft skuteczne wdrożenie systemu ochrony cyberprzestrzeni wymaga bieżącej współpracy państwowych i prywatnych uczestników tego systemu. W związku z powyższym konieczne jest:
   - zidentyfikowanie operatorów (właścicieli) krytycznej infrastruktury i usług w państwie;
   - zidentyfikowanie podmiotów państwowych realizujących zadania w zakresie ochrony cyberprzestrzeni;
   - ustanowienie mechanizmów współdziałania podmiotów państwowych i prywatnych;
   - włączenie państwowych i prywatnych podmiotów w cały proces tworzenia narodowej strategii ochrony cyberprzestrzeni, co zapewni ich odpowiednie zaangażowanie i współpracę;
   - określenie wkładu poszczególnych uczestników w realizację strategii;
   - przypisanie instytucjom państwowym roli *pośrednika*, podmiotu porządkującego i ułatwiającego współpracę na poziomie ogólnonarodowym – np. zapewniającego przepływ informacji, zbierającego ogólnonarodowe wyniki analizy ryzyka;
   - zaangażowanie najwyższych rangą przedstawicieli uczestników (podmiotów realizujących strategię) w celu wykreowania poczucia odpowiedzialności za ten proces;
   - zaangażowanie istniejących zespołów CERT;
   - bezpośrednie zaangażowanie przedstawicieli poszczególnych operatorów (właścicieli) infrastruktury krytycznej (np. firm), a nie tylko przedstawicieli poszczególnych sektorów, co powoduje zwiększenie poczucia odpowiedzialności za proces;
   - zaangażowanie indywidulanych (prywatnych) użytkowników cyberprzestrzeni, w szczególności poprzez zwiększanie ich świadomości zagrożeń.
5. **Ustanowienie precyzyjnej struktury zarządzania krajowym systemem ochrony cyberprzestrzeni,** tj. określenie jasnego systemu ról, zadań i odpowiedzialności wszystkich istotnych uczestników tego procesu. W ramach ww. zadania wytyczne ENISA i Microsoft wskazują na potrzebę:

- wyznaczenia podmiotu publicznego, będącego głównym krajowym koordynatorem strategii ochrony cyberprzestrzeni (np. zespół międzyresortowy, koordynator wskazany przez Premiera/Prezydenta) oraz precyzyjnego opisania jego struktur i zasobów;
- wyznaczenia podmiotu doradczego współpracującego z koordynatorem (np. narodowa rada bezpieczeństwa cybernetycznego) obejmującego szeroką reprezentację uczestników procesu (w tym koniecznie przedstawicieli sektora prywatnego) oraz określenie mandatu i zadań ciała doradczego;
- określenia mandatu i zadań jednostek odpowiedzialnych za: zbieranie informacji dotyczących zagrożeń i podatności, odpowiadających na ataki, realizujących zarządzanie kryzysowe, itd. oraz określenie zasad ich współpracy i komunikacji z ciałem doradczym;
- analizy i zdefiniowania roli CERTów funkcjonujących w sektorze prywatnym i rządowym.

6. **Ustanowienie bezpiecznych i zaufanych mechanizmów wymiany informacji między prywatnymi i publicznymi uczestnikami systemu ochrony cyberprzestrzeni**. Zgodnie z wytycznymi ENISA i Microsoft wymiana informacji między podmiotami prywatnymi i państwowymi stanowi podstawę skutecznego wdrażania narodowej strategii ochrony cyberprzestrzeni. Operatorzy infrastruktury krytycznej mogliby dostarczać instytucjom państwowym dane dotyczące występujących ryzyk, zagrożeń, podatności, podczas gdy podmioty państwowe powinny dostarczać informacje dotyczące globalnych zagadnień bezpieczeństwa narodowego, np. dane uzyskane przez wywiad, policję, itd. Połączenie dwóch ww. źródeł informacji zapewniłoby kompleksowe spojrzenie na kwestię zagrożeń i cyberbezpieczeństwa.

Kluczowe zadania w ramach konstruowania systemu wymiany informacji obejmują:

- zdefiniowanie mechanizmów i reguł systemu wymiany informacji;
- zorganizowanie sektorowych punktów wymiany informacji np. dla energetyki, telekomunikacji, itp.;
- wspieranie wymiany informacji w ramach poszczególnych sektorów, między prywatnymi uczestnikami systemu;
- weryfikowanie, czy osoby uczestniczące w procesie wymiany informacji mają wystarczające kwalifikacje;
- regularne organizowanie bezpośrednich spotkań i utrzymywanie relatywnie wąskiego kręgu uczestników systemu informacji w celu wzbudzenia większego zaufania.

Wytyczne Microsoft podkreślają, że system wymiany informacji musi zapewniać uczestnikom bezzwłocznie informacje na temat nowo pojawiających się zagrożeń i podatności. Wskazują również, że powinien być on koordynowany przez posiadający właściwe uprawnienia organ państwowy.

7. **Rozwój narodowych planów kryzysowych – ciągłości działania** obejmujących reagowanie na poważne incydenty dotyczące krytycznej infrastruktury informatycznej oraz przywracanie ich normalnego funkcjonowania. Narodowy plan ciągłości działania infrastruktury informatycznej powinien być elementem krajowego systemu zarządzania kryzysowego i integralną częścią strategii ochrony cyberprzestrzeni. Celami planu są:
   - określenie kryteriów służących zdefiniowaniu sytuacji jako kryzysowa;

- zdefiniowanie głównych procesów i zadań związanych z zarządzaniem kryzysem;
- precyzyjne określenie zadań poszczególnych uczestników podczas kryzysu cybernetycznego.

Zgodnie z wytycznymi ENISA, przygotowywanie planów kryzysowych dotyczących funkcjonowania cyberprzestrzeni jest zadaniem ciągłym, obejmującym w szczególności: szacowanie ryzyk, zagrożeń, podatności i potencjalnych skutków, przypisanie ról uczestnikom i opracowanie procedur do zastosowania w różnych sytuacjach kryzysowych, szkolenie personelu, testowanie, ćwiczenia i ulepszanie opracowanych schematów działania w wyniku wniosków z przeprowadzonych testów.

8. **Organizacja ćwiczeń systemu bezpieczeństwa cyberprzestrzeni** pozwalających na testowanie procedur awaryjnych, kanałów wymiany informacji, wykrywanie słabości systemu oraz poprawę współpracy między poszczególnymi sektorami i uczestnikami (państwowymi i prywatnymi). W celu organizacji ćwiczeń zasadne jest np. utworzenie *narodowego zespołu* odpowiadającego za ich planowanie. Ćwiczenia powinny mieć sprecyzowane cele, tj. obejmować sprawdzenie funkcjonowania konkretnych elementów planu ciągłości działania infrastruktury informatycznej oraz strategii ochrony cyberprzestrzeni.
9. **Ustanowienie podstawowych wymogów w zakresie bezpieczeństwa cyberprzestrzeni,** tj. minimalnego poziomu bezpieczeństwa dla różnych sektorów publicznych i prywatnych, bazujących na wynikach przeprowadzonej wcześniej analizy ryzyka (uwzględniając różnice między tymi sektorami w profilach ich działania, możliwości finansowe itd.). Zadania realizowane w związku z opracowywaniem wymogów obejmują m.in.: identyfikację istniejących już zabezpieczeń i występujących w nich luk, propozycje poprawy standardów bezpieczeństwa w oparciu o opinie ekspertów i istniejące normy (ISO, COBIT, ITIL) oraz w wyniku analizy występujących incydentów. Zgodnie z wytycznymi Microsoft, zalecenia w zakresie bezpieczeństwa powinny obejmować nie tylko infrastrukturę krytyczną i systemy rządowe, ale również pozostałych użytkowników cyberprzestrzeni (małe firmy, osoby prywatne), którzy również mają wpływ na poprawę ogólnego poziomu bezpieczeństwa cyberprzestrzeni państwa.
10. **Ustanowienie systemu raportowania o incydentach.** Zadania związane z budową systemu obejmują m.in.:
    - sprawdzenie czy funkcjonują już jakieś procedury raportowania o incydentach i określenie ewentualnych potrzeb w zakresie ich rewizji i uzupełnienia;
    - określenie rodzajów incydentów, które powinny podlegać raportowaniu oraz struktury raportowania (kto-komu);
    - określenie procedur raportowania, tj. określenie hierarchii (katalogu incydentów) i wprowadzenie obowiązku zgłaszania dla konkretnych grup incydentów[131].
11. **Ustanowienie systemu reagowania na incydenty w cyberprzestrzeni.**

Zgodnie z wytycznymi ENISA i Microsoft, kluczową rolę w koordynowaniu zarządzania incydentami przez uczestników systemu ochrony cyberprzestrzeni odgrywają **narodowe/rządowe zespoły CERT.** Zakres zadań takiego zespołu obejmuje trzy główne obszary:

[131] Przykładem w ww. zakresie może być procedura postępowania w sytuacji wystąpienia incydentów określona w łotewskiej ustawie dotyczącej bezpieczeństwa technologii informacyjnych z 2010 r., która nakłada na administrację państwową, samorządową i operatorów (właścicieli) infrastruktury krytycznej obowiązek informowania o incydentach narodowego zespołu CERT. W przypadku incydentów zagrażających bezpieczeństwu państwa, zespół CERT informuje kolejne instytucje, w tym Ministra Transportu, właściwego ministra odpowiadającego za dany sektor gospodarki oraz organy bezpieczeństwa państwa.

- zarządzanie incydentami (wspieranie zarządzania incydentami) dotyczącymi sieci i systemów na terenie danego państwa;
- ochronę krytycznej infrastruktury informatycznej państwa;
- wykonywanie zadań krajowego punktu kontaktowego umożliwiającego m.in. wymianę informacji z narodowymi zespołami CERT z innych państw.

Potencjalnymi odbiorcami usług narodowego/rządowego zespołu CERT są wszyscy użytkownicy i administratorzy cyberprzestrzeni z danego państwa, którzy zależnie od zakresu odpowiedzialności i usług świadczonych przez CERT mogą być podzieleni na trzy główne grupy:

- **instytucje rządowe i inne podmioty publiczne**, wobec których narodowy/rządowy CERT świadczy nieograniczony zakres usług;
- **operatorzy infrastruktury krytycznej** – zakres usług świadczonych w stosunku do tych podmiotów będzie zależał od faktu, czy posiadają one swoje własne wyspecjalizowane służby odpowiadające za bezpieczeństwo IT. W takim przypadku, zadania narodowego/rządowego CERT będą polegać przede wszystkim na koordynowaniu i wspieraniu działań tych jednostek. Należy jednak podkreślić, że niezależnie od zakresu usług świadczonych przez narodowy/rządowy CERT wobec operatorów infrastruktury krytycznej, musi istnieć precyzyjnie określona struktura współpracy i komunikacji między tymi podmiotami. Ponadto narodowy/rządowy CERT powinien być zaangażowany w proces budowy systemu zarządzania kryzysowego państwa, tj. w szczególności brać aktywny udział w identyfikacji informatycznej infrastruktury krytycznej oraz w szacowaniu ryzyk dla tej infrastruktury;
- **pozostali użytkownicy i administratorzy cyberprzestrzeni** – zakres usług świadczonych wobec tej grupy przez narodowy/rządowy CERT jest ograniczony jego zasobami. W przypadku stwierdzenia, że dany incydent wykracza poza zakres działalności zespołu, jego załatwienie może być przekazane właściwemu podmiotowi (np. komercyjnemu/branżowemu zespołowi CERT).

Niezależnie od przedstawionego powyżej podziału, specjalna rola narodowego/rządowego zespołu CERT wynika również z faktu, że wykonuje on zadania **krajowego punktu kontaktowego ds. wymiany informacji z narodowymi zespołami CERT z innych państw**. Oznacza to, że narodowy/rządowy CERT odpowiada za przekazywanie informacji o incydentach do innych właściwych organów państwowych. Powinien także zarządzać incydentami, które (np. z powodu wątpliwości kompetencyjnych, czy niewystarczających zasobów) nie zostały załatwione przez inne, krajowe zespoły CERT.

W celu zapewnienie skutecznej realizacji zadań, państwa powinny wyposażyć narodowe/rządowe Zespoły CERT w odpowiednie zasoby oraz określić dla nich[132]:

[132] Na podstawie obowiązującej na Łotwie ustawy dotyczącej bezpieczeństwa technologii informacyjnych z 2010 r. powołany został narodowy CERT (Security Incidents Response Institution), który jest obsługiwany przez krajowego regulatora w obszarze komunikacji oraz Instytut Matematyki i Informatyki Uniwersytetu Łotewskiego. Zadania ww. podmiotu obejmują: koordynację działań prewencyjnych w zakresie ochrony cyberprzestrzeni, publikowanie wytycznych w zakresie bezpieczeństwa bazujących na aktualnej analizie zagrożeń, realizację programów badawczych, edukacyjnych, szkoleń, sprawowanie nadzoru nad przestrzeganiem ustawy dotyczącej bezpieczeństwa technologii informacyjnych przez rząd, samorządy, dostawców usług telekomunikacyjnych oraz współpraca międzynarodowa. Narodowy CERT Łotwy jest uprawniony do: żądania od podmiotów państwowych, samorządowych i prywatnych osób prawnych informacji na temat incydentów, wykonywania testów systemów informatycznych infrastruktury krytycznej oraz wydawania decyzji administracyjnych w stosunku do podmiotów państwowych, samorządowych i prywatnych osób prawnych.

a) **Mandat i strategię**, tj. uprawnienia i kompetencje danego zespołu CERT. Zgodnie z rekomendacjami ENISA:
   - uprawnienia i kompetencje narodowego/rządowego CERT powinny być precyzyjnie opisane w narodowej strategii ochrony cyberprzestrzeni;
   - narodowy/rządowy zespół CERT powinien posiadać formalnie nadany mandat, wyczerpująco i jasno określający zadania, zakres odpowiedzialności oraz odbiorców jego usług;
   - mandat zespołu CERT powinien być publicznie ogłoszony;
   - w przypadku występowania w danym państwie kilku narodowych/rządowych zespołów CERT kluczowe znaczenie ma unikanie nakładania zadań i precyzyjne określenie mandatów tych zespołów;
   - powinna być prowadzona bieżąca ewaluacja (zarówno wewnątrz zespołu jak i w konsultacji z jego otoczeniem zewnętrznym, np. klientami) pozwalająca na ocenę adekwatności mandatu danego zespołu CERT.

b) **Zakres działalności**, tj. katalog usług realizowanych przez dany Zespół dla jego klientów. Zgodnie z rekomendacjami ENISA powinien on obejmować w szczególności:
   - **działania prewencyjne** mające na celu poprawę bezpieczeństwa infrastruktury informatycznej, zapobieganie incydentom i minimalizowanie ich ewentualnych skutków (monitorowanie i wymiana informacji na temat bezpieczeństwa IT, ocena poziomu zabezpieczeń i podatności, wydawanie wytycznych w zakresie zabezpieczeń IT, budowa systemów wczesnego ostrzegania);
   - **reagowanie na incydenty i zagrożenia** (zarządzanie incydentami, alarmowanie i wydawanie komunikatów o zagrożeniach, zarządzanie podatnościami, poszukiwanie luk w systemach i identyfikowanie złośliwego oprogramowania);
   - **pozostałe usługi wpływające na podniesienie ogólnego poziomu bezpieczeństwa** (np. organizowanie kampanii społecznych uświadamiających zagrożenia IT, organizowanie ćwiczeń, opracowywanie planów zarządzania kryzysowego odnośnie krajowej krytycznej infrastruktury informatycznej).

c) **Wymagania organizacyjne**, tj. techniczne, kadrowe i operacyjne wymagania dla danego zespołu. Zgodnie z rekomendacjami ENISA:
   - zasoby (ludzkie, finansowe, sprzętowe) narodowego/rządowego zespołu CERT muszą być adekwatne do przypisanych mu zadań, wynikających z określonego mandatu oraz pozwalać na efektywne działanie w sytuacjach kryzysowych;
   - narodowy/rządowy zespół CERT powinien świadczyć usługi 24 godziny na dobę przez 7 dni w tygodniu;
   - niezbędne jest ustanowienie kliku alternatywnych (zabezpieczonych) kanałów komunikacji z zespołem i udostępnienie informacji na ten temat współpracownikom i potencjalnym klientom;
   - zespół CERT powinien posiadać system ewidencjonowania i śledzenia stanu incydentów;
   - konieczne jest wdrożenie standardowych procedur działania zespołu;
   - zespół CERT powinien opracować i na bieżąco monitorować wskaźniki realizacji głównych zadań, np. czas reakcji na incydent.

d) Zdolności w zakresie współpracy, tj. wymogi dotyczące wymiany informacji z innymi zespołami typu CERT oraz pozostałymi użytkownikami i administratorami cyberprzestrzeni. Zgodnie z rekomendacjami ENISA:

- wymagane jest upowszechnianie wśród użytkowników i administratorów cyberprzestrzeni informacji na temat istnienia i zadań narodowego/rządowego zespołu CERT;
- występuje potrzeba zmian prawnych nakładających obowiązek (np. na przedsiębiorców telekomunikacyjnych, dostawców usług internetowych) przekazywania do narodowego/rządowego zespołu CERT informacji na temat incydentów;
- zespół CERT powinien mieć dostęp do danych dot. naruszeń bezpieczeństwa zbieranych od przedsiębiorców telekomunikacyjnych przez narodowy organ regulacyjny (w Polsce UKE);
- rządowy/narodowy zespół CERT powinien aktywnie współpracować z partnerami międzynarodowymi (np. fora współpracy narodowych zespołów CERT), regionalnymi i krajowymi (Policja, przedsiębiorcy telekomunikacyjni, operatorzy infrastruktury krytycznej, dostawcy usług internetowych itd.);
- w celu usprawnienia współpracy z ww. podmiotami powinny być tworzone różne fora konsultacyjne oraz kanały wymiany informacji. Dobrą praktyką stosowaną przez większość zespołów CERT jest również podpisywanie umów i porozumień, o współpracy, które w pewnej mierze rekompensują brak kompleksowych regulacji prawnych (np. porozumienie o współpracy narodowego/rządowego zespołu CERT z Policją).

Zgodnie z Wytycznymi ENISA i Microsoft krajowy system reagowania na incydenty w cyberprzestrzeni powinien bazować na **katalogu incydentów**, rozumianym jako oznaczenie ich wagi (tj. poziomu zagrożenia – np. incydent kluczowy dla bezpieczeństwa narodowego) wraz ze wskazaniem podmiotu zobowiązanego do reagowania oraz procedur działania. Wymagane jest również określenie roli administracji państwowej w zakresie reagowania na incydenty kluczowe dla bezpieczeństwa narodowego związane z prywatną infrastrukturą krytyczną. Zadania państwa w ww. zakresie mogą przybierać różną postać (np. bezpośrednia obrona, pośrednie wsparcie) zależnie od panującego w danym państwie modelu relacji między prywatnymi operatorami infrastruktury krytycznej a rządem. Jako zasadne wskazano także zainicjowanie narodowego projektu budowy **systemu wczesnego ostrzegania dla krytycznej infrastruktury informatycznej**, który ma oddziaływać m.in. jako forum wzmacniania bieżącej współpracy między różnymi podmiotami państwowymi i prywatnymi.

12. Wspieranie szkoleń i programów edukacyjnych, w związku z niewystarczającą liczbą ekspertów w zakresie ochrony cyberprzestrzeni. Główne zadania w tym obszarze obejmują:

- opracowanie narodowych programów kształcenia i praktyk w obszarze ochrony cyberprzestrzeni;
- wspieranie certyfikacji personelu zajmującego kluczowe stanowiska związane z ochroną cyberprzestrzeni;
- określenie katalogu funkcji osób odpowiedzialnych za ochronę cyberprzestrzeni i przypisanie do tych zadań adekwatnych wymogów dotyczących wykształcenia i kwalifikacji[133];

[133] Formalny system kształcenia i certyfikacji uprawnień został wprowadzony np. na podstawie obowiązującej na Łotwie ustawy dotyczącej państwowych systemów informatycznych z 2002 r. w przypadku tzw. menadżerów bezpieczeństwa państwowych systemów informatycznych.

- wprowadzenie elementów wiedzy z zakresu cyberbezpieczeństwa do różnych programów studiów (nie tylko studiów informatycznych);
- stworzenie krajowego rejestru akredytowanych wykładowców posiadających odpowiednie kwalifikacje w zakresie ochrony cyberprzestrzeni.

13. **Zwiększanie poziomu świadomości indywidulanych i korporacyjnych użytkowników cyberprzestrzeni** m.in. poprzez prowadzenie kampanii informacyjno-edukacyjnych.
14. **Wspieranie badań i rozwoju w obszarze ochrony cyberprzestrzeni.**
    - konieczność takich działań powinna być podkreślona w narodowej strategii ochrony cyberprzestrzeni;
    - stworzenie forum pozwalającego na wymianę informacji o możliwościach i potrzebach pomiędzy przemysłem i administracją.
15. **Zwalczanie przestępczości w cyberprzestrzeni poprzez:**
    - wprowadzenie wymaganych regulacji prawnych i ratyfikację istniejących traktatów międzynarodowych;
    - powołanie specjalnych państwowych organów odpowiadających za zwalczanie przestępczości w sieci;
    - zapewnienie ciągłych, specjalistycznych szkoleń dla policjantów i sędziów.
16. **Zaangażowanie we współpracę międzynarodową.**
    - aktywna identyfikacja krajów, z którymi chce się nawiązać współpracę poprzez składanie propozycji zawierających przyczyny i cel współpracy;
    - wyznaczenie jednej krajowej organizacji jako odpowiedzialnej za promowanie i wsparcie organizacyjne takiej współpracy;
    - udział w regionalnych, europejskich i międzynarodowych ćwiczeniach dla intensyfikacji współpracy z partnerami strategicznymi.

Zgodnie z wytycznymi ENISA i Microsoft, warunkiem skutecznego wdrażania narodowej strategii w zakresie ochrony cyberprzestrzeni jest bieżące monitorowanie stopnia realizacji zapisanych w tym dokumencie celów. Ewaluacja efektywności strategii powinna być prowadzona bezpośrednio od momentu rozpoczęcia jej wdrażania przy wykorzystaniu precyzyjnie zdefiniowanych wskaźników realizacji zadań.

Wykaz osób zajmujących w okresie objętym kontrolą stanowiska kierownicze w badanych jednostkach

Lp.	Osoby kierujące kontrolowaną działalnością		Okres sprawowania funkcji
1.	**Minister Administracji i Cyfryzacji**	Michał Boni	18.11.2011 r . – 27.11.2013 r.
		Rafał Trzaskowski	03.12.2013 r. – 22.09.2014 r.
		Andrzej Halicki	22.09.2014 r. – obecnie
2.	**Dyrektor Rządowego Centrum Bezpieczeństwa**	Antoni Podolski	02.08.2008 r. – 01.09.2009 r.
		Przemysław Guła (pełniący obowiązki)	22.09.2009 r. – 28.12.2009 r.
		Marcin Samsonowicz-Górski	29.12.2009 r. – 21.12.2010 r.
		Marek Komorowski (pełniący obowiązki)	22.12.2010 r. – 14.06.2012 r.
		Marek Komorowski	15.06.2012 r. – 14.04.2014 r.
		Krzysztof Malesa (pełniący obowiązki)	15.04.2014 r. – 28.04.2014 r.
		Janusz Skulich	29.04.2014 r. – obecnie
3.	**Minister Spraw Wewnętrznych**	Jacek Cichocki	18.11.2011 r. – 25.02.2013 r.
		Bartłomiej Sienkiewicz	25.02.2013 r. – do końca okresu objętego kontrolą
4.	**Minister Obrony Narodowej**	Bogdan Klich	16.11.2007 r. – 02.08.2011 r.
		Tomasz Siemoniak	02.08.2011 r. – obecnie
5.	**Komendant Główny Policji**	nadinsp. Tadeusz Budzik	08.08.2007 r. – 05.03.2008 r.
		gen. insp. Andrzej Matejuk	06.03.2008 r. – 09.01.2012 r.
		gen. insp. Marek Działoszyński	10.01.2012 r. – do końca okresu objętego kontrolą
6.	**Dyrektor Naukowej i Akademickiej Sieci Komputerowej**	Maciej Kozłowski	28.10.2005 r. – 15.11.2009 r.
		Michał Chrzanowski	16.11.2009 r. – obecnie
7.	**Szef Agencji Bezpieczeństwa Wewnętrznego**	Krzysztof Bondaryk	16.11.2007 r. – 15.01.2013 r.
		płk Dariusz Łuczak (pełniący obowiązki)	16.01.2013 r. – 15.04.2013 r.
		płk Dariusz Łuczak	16.04.2013 r. – obecnie
8.	**Prezes Urzędu Komunikacji Elektronicznej**	Anna Streżyńska	14.01.2006 r. – 26.01.2012 r.
		Magdalena Gaj	27.01.2012 r. – obecnie

Wykaz podstawowych aktów prawnych dotyczących kontrolowanej działalności

1. Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. (Dz. U. Nr 78, poz. 483 ze zm.)
2. Ustawa z dnia 29 sierpnia 2002 r. o stanie wojennym oraz o kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej (Dz. U. z 2014 r., poz. 1815).
3. Ustawa z dnia 21 czerwca 2002 r. o stanie wyjątkowym (Dz. U. z 2014 r., poz. 1191).
4. Ustawa z dnia 18 kwietnia 2002 r. o stanie klęski żywiołowej (Dz. U. z 2014 r., poz. 333 ze zm.).
5. Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2014 r., poz. 1114).
6. Ustawa z dnia 12 lutego 2010 r. o zmianie ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne oraz niektórych innych ustaw (Dz. U. Nr 40, poz. 230).
7. Ustawa z dnia 16 lipca 2004 r. Prawo telekomunikacyjne (Dz. U. z 2014 r., poz. 243 ze zm.).
8. Ustawa z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (Dz. U. z 2013 r., poz. 1422).
9. Ustawa z dnia 29 sierpnia 1997 r. Prawo bankowe (Dz. U. z 2015, poz. 128).
10. Ustawa z dnia 18 września 2001 r. o podpisie elektronicznym (Dz. U. z 2013 r., poz. 262 ze zm.).
11. Ustawa z dnia 4 września 1997 r. o działach administracji rządowej (Dz. U. Nr 2013, poz. 743 ze zm.).
12. Ustawa z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu (Dz. U. z 2010 r. Nr 29, poz. 154 ze zm.).
13. Ustawa z dnia 6 kwietnia 1990 r. o Policji (Dz. U. z 2015 r., poz. 355).
14. Ustawa z dnia 30 kwietnia 2010 r. o instytutach badawczych (Dz. U. Nr 96, poz. 618 ze zm.).
15. Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz. U. z 2013 r., poz. 1166).
16. Ustawa z dnia 8 sierpnia 1996 r. o Radzie Ministrów (Dz. U. z 2012 r., poz. 392 ze zm.).
17. Rozporządzenie 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).
18. Rozporządzenie Prezesa Rady Ministrów z dnia 22 września 2014 r. w sprawie szczegółowego zakresu działania Ministra Spraw Wewnętrznych (Dz. U. z 2014 r., poz. 1265).
19. Rozporządzenie Rady Ministrów z dnia 9 lipca 1996 r. w sprawie szczegółowego zakresu działania Ministra Obrony Narodowej (Dz. U. Nr 94, poz. 426 ze zm.).
20. Rozporządzenie Rady Ministrów z dnia 4 stycznia 2010 r. w sprawie planu działań przedsiębiorcy telekomunikacyjnego w sytuacjach szczególnych zagrożeń (Dz. U. Nr 15, poz. 77).
21. 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 ze zm.).
22. Rozporządzenie Rady Ministrów z dnia 30 kwietnia 2010 r. w sprawie Raportu o zagrożeniach bezpieczeństwa narodowego (Dz. U. Nr 83, poz. 540).
23. Rozporządzenie Rady Ministrów z dnia 30 kwietnia 2010 r. w sprawie Narodowego Programu Ochrony Infrastruktury Krytycznej (Dz. U. Nr 83, poz. 541).

24. Rozporządzenie Rady Ministrów z dnia 30 kwietnia 2010 r. w sprawie planów ochrony infrastruktury krytycznej (Dz. U. Nr 83, poz. 542).
25. Rozporządzenie Rady Ministrów z dnia 4 października 2010 r. w sprawie wykazu przedsiębiorców o szczególnym znaczeniu gospodarczo-obronnym (Dz. U. z 2014 r., poz. 303 ze zm.).
26. Uchwała Nr 190 Rady Ministrów z dnia 29 października 2013 r. Regulamin pracy Rady Ministrów (M.P. z 2013 r., poz. 979).
27. Decyzja Nr 243/MON Ministra Obrony Narodowej z dnia 18 czerwca 2014 r. w sprawie organizacji i funkcjonowania systemu reagowania na incydenty komputerowe w resorcie obrony narodowej (Dz. Urz. MON z 2014 r., poz. 203).
28. Decyzja Nr 38/MON Ministra Obrony Narodowej z dnia 16 lutego 2012 r. w sprawie powołania Pełnomocnika Ministra Obrony Narodowej ds. Bezpieczeństwa Cyberprzestrzeni (Dz. Urz. MON z 2012 r., poz., 52 ze zm.).
29. Zarządzenie Nr 10/MON Ministra Obrony Narodowej z dnia 29 kwietnia 2013 r. w sprawie utworzenia i nadania statutu państwowej jednostce budżetowej - Narodowe Centrum Kryptologii (Dz. Urz. MON z 2013 r., poz. 121 ze zm.).
30. Zarządzenia Nr 8 Komendanta Głównego Policji z dnia 15 marca 2013 r. w sprawie regulaminu Komendy Głównej Policji (Dz. Urz. KGP z 2013 r., poz. 25 ze zm.).
31. Dyrektywa Parlamentu Europejskiego i Rady 2013/40/UE z dnia 12 sierpnia 2013 r. dotycząca ataków na systemy informatyczne i zastępująca decyzję ramową Rady 2005/222/WSiSW (Dz.U. L 218 z 12.08.2013 s.8.).
32. Konwencja Rady Europy o cyberprzestępczości z dnia 23 listopada 2001 r.

Wykaz organów, którym przekazano informację o wynikach kontroli

1. Prezydent Rzeczypospolitej Polskiej
2. Marszałek Sejmu Rzeczypospolitej Polskiej
3. Marszałek Senatu Rzeczypospolitej Polskiej
4. Prezes Rady Ministrów Rzeczypospolitej Polskiej
5. Prezes Trybunału Konstytucyjnego
6. Rzecznik Praw Obywatelskich
7. Minister Obrony Narodowej
8. Minister Administracji i Cyfryzacji
9. Minister Spraw Wewnętrznych
10. Prokurator Generalny
11. Komendant Główny Policji
12. Szef Agencji Bezpieczeństwa Wewnętrznego
13. Prezes Urzędu Komunikacji Elektronicznej
14. Dyrektor Rządowego Centrum Bezpieczeństwa
15. Sejmowa Komisja Administracji i Cyfryzacji
16. Sejmowa Komisja Innowacyjności i Nowoczesnych Technologii
17. Sejmowa Komisja Obrony Narodowej
18. Sejmowa Komisja Spraw Wewnętrznych
19. Sejmowa Komisja do Spraw Kontroli Państwowej

Warszawa, dnia 10 lipca 2015 r.

RZECZPOSPOLITA POLSKA
MINISTERSTWO
ADMINISTRACJI I CYFRYZACJI

PODSEKRETARZ STANU
Jurand Drop

DSI-WBC.0810.1.2015

Pan
Wojciech Kutyła
Wiceprezes
Najwyższej Izby Kontroli

W odpowiedzi na pismo z dnia 26 czerwca 2015 r. znak: KPB-4101-002-00/2014, zawierające *Informację o wynikach kontroli „Realizacja przez podmioty państwowe zadań w zakresie ochrony cyberprzestrzeni Rzeczypospolitej Polskiej"* (dalej: *Informacja*) pragnę przedstawić uzupełniające informacje ze strony Ministerstwa Administracji i Cyfryzacji (MAiC).

Prowadzenie koordynacji polityki cyberbezpieczeństwa, czyli problemu dotyczącego wszystkich sektorów gospodarki i życia publicznego, jest długotrwałym i skomplikowanym procesem, wymagającym wieloletniego zaangażowania wielu podmiotów, wysoce wykwalifikowanych kadr oraz odpowiednich funduszy. Szybkość przygotowania i przyjęcia *„Polityki Ochrony Cyberprzestrzeni RP"* (dalej: *Polityka*) uniemożliwiła przeprowadzenie kluczowych analiz w procesie przygotowawczym, i z tego powodu wiele działań analitycznych, w tym przygotowanie planu konkretnych działań, musiało nastąpić w okresie późniejszym.

Od połowy 2013 r. MAiC prowadziło działania zgodnie z zapisami *Polityki,* ukierunkowane na rozwój i wzmacnianie systemu ochrony cyberprzestrzeni Polski, przygotowując konkretne działania, które miała podjąć administracja publiczna. Nie było to łatwe, gdyż jak słusznie zauważono w *Informacji*, brak wskazania na poziomie norm prawnych jednego ośrodka decyzyjnego, koordynującego działania innych instytucji publicznych i – co najważniejsze – posiadającego uprawnienia w zakresie oddziaływania na te inne instytucje był kluczowym czynnikiem uniemożliwiającym sprawne działanie.

Niemniej jednak MAiC dokładało wysiłków, by wypełnić zadania wynikające z *Polityki* w najlepszy sposób, jak był możliwy. W tym celu w czerwcu 2014 r. przy Komitecie Rady Ministrów ds. Cyfryzacji (KRMC) powołano Zespół zadaniowy ds. bezpieczeństwa cyberprzestrzeni Rzeczypospolitej Polskiej. Na jego forum prowadzono regularne prace, których wynikiem było uzgodnienie *„Planu działań w zakresie zapewnienia bezpieczeństwa cyberprzestrzeni RP"*. Został on przyjęty 13 kwietnia br. przez Komitet Rady Ministrów ds. Cyfryzacji i obecnie jest wdrażany życie.

W poruszonej w *Informacji* kwestii „biernego oczekiwania na rozwiązania, które w tym obszarze zaproponuje Unia Europejska" warto zauważyć, iż przyjęcie *dyrektywy w sprawie środków mających na celu zapewnienie wspólnego wysokiego poziomu bezpieczeństwa sieci i informacji w obrębie Unii* (dyrektywa NIS) będzie się wiązać z koniecznością istotnych zmian w prawie krajowym. MAiC bierze aktywny udział w negocjacjach na poziomie europejskim, by ostateczne rozwiązanie w optymalny sposób odpowiadało potrzebom Polski. Implementacja dyrektywy będzie okazją do wprowadzenia przemyślanych zmian do polskiego porządku prawnego.

Odnosząc się do konkretnych wniosków pokontrolnych, skierowanych do MAiC i przedstawionych w *Informacji* na str. 73, należy przekazać następujące informacje.

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.*

Ministerstwo Administracji i Cyfryzacji na bieżąco prowadzi analizę istniejących dokumentów strategicznych, programowych i regulacji prawnych dotyczących ochrony cyberprzestrzeni. Polska podobnie jak niektóre kraje europejskie (Finlandia, Francja, Węgry) przyjęła ustawę i inne akty prawne określające minimalne wymagania z zakresu bezpieczeństwa teleinformatycznego w administracji publicznej (ustawa o ustawie z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne[1], oraz 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[2]).

[1] Dz. U. z 2014 r., poz. 1114 z późn. zm.
[2] Dz. U. z 2012 r. Nr 526 z późn. zm.

Minister Administracji i Cyfryzacji nadzoruje też Urząd Komunikacji Elektronicznej, do którego zgłaszane są zgodnie z ustawą z dnia 16 lipca 2004 r. *Prawo telekomunikacyjne*[3] najważniejsze incydenty cybernetyczne w sieciach telekomunikacyjnych. Minister Administracji i Cyfryzacji pełni również w imieniu Rady Ministrów koordynacyjną rolę w zakresie realizacji *Polityki*.

Działania samoregulacyjne odnoszące się do sfery infrastruktury krytycznej są koordynowane przez Rządowe Centrum Bezpieczeństwa (RCB), które zgodnie z ustawą o zarządzaniu kryzysowym i Narodowym Programie Ochrony Infrastruktury Krytycznej (NPOIK) weryfikuje plany operatorów infrastruktury krytycznej m.in. pod kątem oceny ryzyka, stosowanych zabezpieczeń i przyjętych w obiektach zasad ochrony teleinformatycznej. RCB jest również odpowiedzialne za inwentaryzację kluczowych, państwowych zasobów IT.

Polityka jest ograniczona do urzędów administracji rządowej, a zatem decyzja dotycząca nowych ram ochrony cyberprzestrzeni obejmujących zarówno sferę administracji publicznej jak i infrastruktury krytycznej może zostać podjęta przez Komitet Rady Ministrów ds. Cyfryzacji, a później przez Radę Ministrów.

Ministerstwo Administracji i Cyfryzacji zleciło w 2015 r. opracowanie ekspertyzy dotyczącej organizacji systemu cyberbezpieczeństwa w Polsce. Ekspertyza, opierając się na obecnym stanie prawnym i istniejących zasobach, określi potrzeby nowych rozwiązań legislacyjnych dotyczących minimalnych wymagań z zakresu bezpieczeństwa w sektorach krytycznych i administracji rządowej oraz sposoby ich wdrażania, jak również wskaże propozycje ram instytucjonalnych podmiotów zajmujących się zarządzaniem bezpieczeństwem cyberprzestrzeni w wymiarze strategicznym i operacyjno-regulacyjnym.

2. *Rzetelne oszacowanie zasobów (ludzkich, finansowych i rzeczowych) Ministerstwa oraz innych instytucji państwowych niezbędnych do budowy i skutecznego funkcjonowania krajowego systemu ochrony cyberprzestrzeni.*

Ministerstwo Administracji i Cyfryzacji przeprowadziło analizę zasobów urzędu, niezbędnych do realizacji zadań wynikających z *Polityki*. Na podstawie jej wniosków jest przygotowywana koncepcja departamentu realizującego zadania koordynacji polityki ochrony cyberprzestrzeni. W dniu 19 czerwca 2015 r. weszło również w życie Zarządzenie Nr 25/2015 Dyrektora Generalnego Ministerstwa Administracji i Cyfryzacji w sprawie zmian regulaminu

[3] Dz. U. z 2014 r. Nr 243 j.t.

organizacyjnego Departamentu Społeczeństwa Informacyjnego MAC, powołujące w ramach departamentu Wydział Bezpieczeństwa Cyberprzestrzeni.

Ponadto w ramach prac prowadzonych nad projektem *„Planu działań w zakresie zapewnienia bezpieczeństwa cyberprzestrzeni RP"* przez Zespół zadaniowy ds. bezpieczeństwa cyberprzestrzeni Rzeczypospolitej Polskiej ministerstwo zwróciło się do wybranych instytucji państwowych związanych z ochroną cyberprzestrzeni o przedstawienie informacji dotyczących niezbędnych zasobów. Konsultowane instytucje nie były w stanie przedstawić danych finansowych bądź wyliczeń, dlatego też wymieniona wcześniej ekspertyza określi m.in. szacunki finansowe scentralizowanego bądź rozproszonego systemu ochrony cyberprzestrzeni.

Ministerstwo Administracji i Cyfryzacji we własnym zakresie opracowało dodatkowo krótką analizę porównawczą dotyczącą systemów cyberbezpieczeństwa w wybranych krajach, jak również zorganizowało w bieżącym roku w Polsce spotkania z przedstawicielami niemieckich i amerykańskich instytucji rządowych nt. organizacji krajowych systemów bezpieczeństwa cyberprzestrzeni.

Na podstawie powyższych prac Ministerstwo Administracji i Cyfryzacji przygotuje oszacowanie zasobów 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.*

Ministerstwo Administracji i Cyfryzacji pragnie podkreślić, że w *Polityce* uwzględniono zadania i role zespołów ds. reagowania na incydenty komputerowe. Kluczowym wyzwaniem z punktu widzenia rozwoju systemu ochrony cyberprzestrzeni RP jest zwiększenie współpracy podmiotów prowadzących działalność operacyjną w zakresie bezpieczeństwa cyberprzestrzeni. Można wskazać, iż oprócz zespołów ds. reagowania na incydenty komputerowe wiele państw z rozwiniętym sektorem teleinformatycznym posiada jednostki, które gromadzą dane o zagrożeniach i podatnościach oraz wydają wytyczne bezpieczeństwa teleinformatycznego[4].

[4] W Niemczech funkcjonuje Federalny Urząd Bezpieczeństwa Informacji, Holandii - Narodowe Centrum Cyberbezpieczeństwa, Wielkiej Brytanii – Biuro Cyberbezpieczeństwa.

Ministerstwo Administracji i Cyfryzacji podjęło prace analityczne nad strategicznym kierunkiem kształtu systemu ochrony cyberprzestrzeni, a elementem ekspertyzy, o której była mowa wcześniej, będzie wariant utworzenia podobnego centrum kompetencyjnego w Polsce. Po przeprowadzeniu niezbędnych prac analitycznych, stosowna informacja zostanie przekazana do Prezesa Rady Ministrów.

4. *Bezzwłoczne 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.*

W kwestiach instytucjonalnych, obecnie funkcjonuje opisany na początku pisma Zespół zadaniowy ds. bezpieczeństwa cyberprzestrzeni Rzeczypospolitej Polskiej przy KRMC i przygotowująca odpowiednie uzgodnienia i dokumenty grupa ekspercka, w skład której wchodzą przedstawiciele MAC, MON, ABW, MIR, RCB, NASK, KGP.

W ramach funkcji koordynacyjnej Ministerstwo Administracji i Cyfryzacji rozwija i upowszechnia przewidzianą *Polityką* sieć pełnomocników ds. bezpieczeństwa teleinformatycznego obejmującą w chwili obecnej 127 pełnomocników w urzędach administracji rządowej. Dla pełnomocników ds. bezpieczeństwa zostały zorganizowane w Warszawie 4 szkolenia specjalistyczne. Dodatkowo Ministerstwo Administracji i Cyfryzacji było współorganizatorem konferencji „*CYBERGOV 2015. Bezpieczeństwo IT w sektorze publicznym*", która odbyła się 18 czerwca br. Ministerstwo Administracji i Cyfryzacji organizowało także konkursy dla organizacji działalności pożytku publicznego, których efektem są liczne materiały edukacyjne, m.in. w zakresie bezpiecznego korzystania z usług elektronicznych. Szansą jest tu także „*Program Operacyjny Polska Cyfrowa na lata 2014-2020"* i przyszłe projekty, które będą dotyczyć m.in. podniesienia poziomu świadomości obywateli w zakresie bezpiecznego korzystania z Internetu oraz usług świadczonych drogą elektroniczną oraz wiedzy o dostępnych narzędziach podnoszących poziom bezpieczeństwa. „*Program Polska Cyfrowa na lata 2014-2020"* umożliwi również budowę/rozbudowę narzędzi technicznych monitorujących w czasie rzeczywistym zagrożenia cyberprzestrzeni w administracji publicznej tzw. usług zdalnego centrum bezpieczeństwa (Security Operations Center), umożliwiających operacyjne zarządzanie incydentem cybernetycznym.

W ramach upowszechnienia istotnych informacji z zakresu bezpieczeństwa sieci i informacji, Ministerstwo Administracji i Cyfryzacji na bieżąco współpracuje z polskim członkiem zarządu w Europejskiej Agencji ds. Bezpieczeństwa Sieci i Informacji, a uzyskane materiały i wytyczne agencji są dystrybuowane wśród pełnomocników ds. bezpieczeństwa cyberprzestrzeni. Przygotowano również dokument *„Rekomendacje dla pełnomocników bezpieczeństwa cyberprzestrzeni RP"*, przeprowadzono szkolenie pracowników urzędów wojewódzkich dotyczące Krajowych Ram Interoperacyjności.

Podsumowując, pragnę zadeklarować, iż kierownictwo Ministerstwa Administracji i Cyfryzacji ma świadomość zadań związanych z *„Polityką Ochrony Cyberprzestrzeni RP"*, jednak szeroko opisane w *Informacji* NIK ograniczenia – w tym szczególnie brak odpowiednich środków finansowych, co przełożyło się ograniczone zasoby kadrowe – nie pozwoliły realizować wszystkich zadań związanych z ochroną cyberprzestrzeni.

Przedstawiając powyższe, uprzejmie proszę o przyjęcie przedłożonych wyjaśnień jako informacji o sposobie wykorzystania uwag i wykonania wniosków pokontrolnych. Dodatkowo, w najbliższym czasie MAC przekaże propozycje działań, które zamierza podjąć w celu realizacji zaleceń Najwyższej Izby Kontroli.

Z poważaniem,

PODSEKRETARZ STANU
w Ministerstwie Administracji i Cyfryzacji
Jurand Drop