Bezpieczeństwo fundamentem działania państwa

Rocznice skłaniają do refleksji, tym bardziej jeśli chodzi o stulecie utworzenia instytucji, której prawne podstawy funkcjonowania zostały wyznaczone przez Konstytucję RP i ustawę o Najwyższej Izbie Kontroli. Nie sposób przy tej okazji nie zadać sobie pytania, na ile działalność kontrolna NIK przyczyniła się do poprawy funkcjonowania państwa. Artykuł koncentruje się na jego szeroko rozumianym bezpieczeństwie wewnętrznym.

MAREK BIEŃKOWSKI

Powołanie departamentu

Pod koniec sierpnia 2011 r. prezes Najwyższej Izby Kontroli określił organizację wewnętrzną i właściwości NIK[1]. Wśród nowo powołanych jednostek organizacyjnych znalazł się Departament Porządku i Bezpieczeństwa Wewnętrznego, któremu przypisano sprawy objęte działami administracji rządowej dotyczące sprawiedliwości i spraw wewnętrznych. Departament objął aż 11 części budżetowych – poczynając od Sądu Najwyższego, przez cywilne służby specjalne, a kończąc na jednostkach organizacyjnych Prokuratury.

Problematyka szeroko rozumianego bezpieczeństwa wewnętrznego państwa jest jednak obecna w działaniach Izby znacznie dłużej. Departament Porządku i Bezpieczeństwa Wewnętrznego przejął bowiem część zadań od swojego poprzednika, tj. od Departamentu Obrony Narodowej i Bezpieczeństwa Wewnętrznego oraz od Departamentu Administracji Publicznej. Z tych dwóch jednostek udało się pozyskać bardzo wartościowych kontrolerów, którzy w większości pracują do dziś.

O sile i znaczeniu jednostek kontrolnych Izby świadczą wyniki kontroli. Departament funkcjonujący w obecnym kształcie ma ich na swoim koncie

[1] Zarządzenie nr 12/2011 Prezesa Najwyższej Izby Kontroli z 29.8.2011 w sprawie szczegółowej organizacji wewnętrznej oraz właściwości jednostek organizacyjnych Najwyższej Izby Kontroli.

ponad czterdzieści, nie licząc corocznych kontroli budżetowych.

W artykule zostaną przedstawione wyniki kilku kontroli, które – moim zdaniem – z uwagi na charakter i wagę ustaleń, w największym stopniu przyczyniły się do poprawy bezpieczeństwa wewnętrznego kraju.

Katastrofa smoleńska

Kontrola „Organizacji wyjazdów i zapewnienia bezpieczeństwa osobom zajmującym kierownicze stanowiska w państwie, korzystającym z lotnictwa transportowego Sił Zbrojnych RP w latach 2005–2010”[2], którą przeprowadzaliśmy jeszcze w strukturach Departamentu Infrastruktury NIK, stała się swoistym kamieniem węgielnym pod budowę przyszłego Departamentu Porządku i Bezpieczeństwa Wewnętrznego. Jej wyniki odbiły się szerokim echem i do dziś są komentowane. Wszystkie zebrane dokumenty przekazaliśmy zarówno do ówczesnej Prokuratury Wojskowej, jak i do Prokuratury Okręgowej w Warszawie, z prośbą o dokonanie analizy prawnokarnej. Dzięki naszym ustaleniom część rodzin ofiar katastrofy pod Smoleńskiem, podczas której na pokładzie samolotu rządowego zginęło 96 osób, w tym Prezydent RP oraz wielu przedstawicieli państwa i różnych organizacji, zdecydowała się skierować prywatne akty oskarżenia[3]. Procesy w tej sprawie trwają do dziś.

Po kontroli, co jest niezwykle rzadkie w praktyce działania Izby, skierowaliśmy wniosek do Ministra Obrony Narodowej o natychmiastowe rozwiązanie 36. Specjalnego Pułku Lotnictwa Transportowego (SPLT). Skala nieprawidłowości i wieloletnich zaniechań była bowiem na niespotykanym poziomie. Dalsze funkcjonowanie 36. SPLT nie gwarantowało prawidłowej realizacji zadań przez tę jednostkę. Minister przychylił się do naszego wniosku.

W czasie kontroli badaliśmy nie tylko przygotowania do lotu z 10 kwietnia 2010 roku, ale objęliśmy nią o wiele dłuższy okres, bo aż od końca 2005 r. Od tego bowiem czasu obowiązywały przepisy, które w zamyśle ich autorów miały gwarantować pełne bezpieczeństwo najważniejszych osób w państwie, korzystających z transportu lotniczego Sił Zbrojnych RP. Chcieliśmy sprawdzić, czy popełnione bardzo poważne błędy w organizacji wylotu premiera 7 kwietnia i prezydenta 10 kwietnia 2010 miały charakter incydentalny, czy też systemowy.

Najwyższa Izba Kontroli negatywnie oceniła realizację przez organy państwa zadań związanych z organizacją wyjazdów i zapewnieniem bezpieczeństwa osobom zajmującym kierownicze stanowiska w państwie, korzystającym z lotnictwa transportowego Sił Zbrojnych RP w latach 2005–2010. We wszystkich kontrolowanych podmiotach stwierdzono

[2] Kontrola: *Organizacja wyjazdów i zapewnienie bezpieczeństwa osobom zajmującym kierownicze stanowiska w państwie, korzystających z lotnictwa transportowego Sił Zbrojnych RP w latach 2005–2010*, nr I/10/001.

[3] Ustalenia kontroli nie dają odpowiedzi na pytanie co było bezpośrednią przyczyną tej katastrofy. To zadanie postawiono Komisji ds. badania wypadków lotniczych i Prokuraturze.

istotne nieprawidłowości, które miały charakter systemowy i występowały w całym okresie objętym kontrolą. Polegały one w szczególności na:

- nieopracowaniu przez podmioty uczestniczące w organizacji przelotów z wykorzystaniem wojskowego specjalnego transportu lotniczego (WSTL) spójnego systemu norm, procedur i zasad postępowania, które skutecznie minimalizowałyby ryzyko wystąpienia sytuacji mogących mieć negatywny wpływ na bezpieczeństwo najważniejszych osób w państwie;
- niewywiązywaniu się przez kolejnych szefów Kancelarii Prezesa Rady Ministrów (KPRM) z obowiązków związanych z organizacją wizyt, w szczególności w zakresie koordynacji wykorzystania WSTL przez osoby uprawnione, w tym składania zamówień na loty;
- nierealizowaniu przez kolejnych ministrów spraw zagranicznych kluczowych zadań w dotyczących przygotowania wizyt, w szczególności niezapewnieniu skutecznego nadzoru nad wypełnieniem procedury uzyskiwania zgód dyplomatycznych na przelot i lądowanie samolotów o statusie HEAD, a także nad organizacją spotkań koordynacyjnych oraz rekonesansów poprzedzających wizyty;
- niereagowaniu lub zbyt późnym reagowaniu przez kolejnych ministrów obrony narodowej i dowódców Sił Powietrznych na niekorzystne zjawiska zachodzące w 36. SPLT oraz braku właściwego nadzoru nad funkcjonowaniem pułku, w tym nad kwestiami bezpieczeństwa lotów;
- braku niezbędnej dla prawidłowego funkcjonowania pułku liczby załóg lotniczych przewożących najważniejsze osoby w państwie, obniżającym się poziomie wyszkolenia załóg statków powietrznych, eksploatacji przestarzałej i awaryjnej techniki lotniczej, lekceważeniu obowiązujących procedur;
- niesporządzaniu przez BOR analiz zagrożeń i planów realizacji działań ochronnych w stosunku do najważniejszych osób w państwie oraz braku systemu nadzoru i kontroli nad przygotowaniem i prowadzeniem tych działań;
- braku nadzoru kolejnych ministrów spraw wewnętrznych i administracji nad działalnością BOR, zwłaszcza w zakresie przygotowania i realizacji działań ochronnych w stosunku do najważniejszych osób w państwie.

W ocenie NIK nieprawidłowości te miały istotny wpływ na niewłaściwą organizację wizyt najważniejszych osób w państwie, a tym samym na ich bezpieczeństwo. Biorąc pod uwagę skalę i rangę nieprawidłowości należy przyjąć, że ryzyko wystąpienia realnego niebezpieczeństwa dla najważniejszych osób w państwie, korzystających z transportu lotniczego Sił Zbrojnych RP było w kontrolowanym okresie wysokie. W mojej ocenie, wyniki tej kontroli stały się swoistą przestrogą na przyszłość.

EURO 2012

Zakończenie kontroli dotyczącej katastrofy pod Smoleńskiem zbiegło się w czasie z powołaniem naszego departamentu. Od początku jego istnienia z gronem moich współpracowników dokonywaliśmy analizy ryzyka powstania nieprawidłowości w tych obszarach, które dotyczyły naszej aktywności kontrolnej. Staraliśmy się również reagować na bieżące problemy, przed którymi stawały służby

odpowiedzialne za bezpieczeństwo wewnętrzne Polski. Wpisywała się w to nasza kontrola dotycząca bezpieczeństwa imprez masowych. Zbadaliśmy „Przygotowanie Polski do organizacji finałowego turnieju Mistrzostw Europy w Piłce Nożnej UEFA EURO 2012"[4] oraz „Gromadzenie, przetwarzanie i udostępnianie informacji dotyczących bezpieczeństwa imprez masowych"[5]. Wyniki ustaleń i wnioski zostały uwzględnione przez służby i instytucje w procesie przygotowań do zabezpieczenia najważniejszej imprezy sportowej w kraju. Ustaliliśmy między innymi, że zakazy stadionowe, orzekane przez sądy wobec najbardziej niebezpiecznych uczestników imprez masowych, docierały do zainteresowanych – w tym Policji – drogą pocztową z wielotygodniowym opóźnieniem, kiedy zawody sportowe, których dotyczył zakaz stadionowy, już dawno przeszły do historii.

W przeprowadzonych kontrolach staraliśmy się podejmować przede wszystkim tematy dotyczące bezpieczeństwa obywateli. W naszej ocenie, należało przyjrzeć się tworzeniu systemu powiadamiania ratunkowego[6], którego wadliwe działanie mogło dotknąć każdego z nas. Nasza ocena była jednoznacznie negatywna, ponieważ nie uruchomiono systemu powiadamiania ratunkowego w kształcie wynikającym z ustawy z 24 sierpnia 1991 r. o ochronie przeciwpożarowej. Nie zakończono procesu tworzenia Centrów Powiadamiania Ratunkowego (CPR) i Wojewódzkich Centrów Powiadamiania Ratunkowego (WCPR), pomimo że dotychczasowe rozwiązania organizacyjne związane z przyjmowaniem i obsługą zgłoszeń o zdarzeniach mogły funkcjonować do czasu utworzenia centrów powiadamiania ratunkowego, jednak nie dłużej niż do 31 grudnia 2011 r.[7] W tym czasie w Ministerstwie Spraw Wewnętrznych i Administracji trwały prace nad opracowaniem projektów aktów prawnych dotyczących systemu powiadamiania ratunkowego, a w szczególności ustawy o powiadamianiu ratunkowym, zmianie ustawy o zarządzaniu kryzysowym oraz zmianie ustawy o ochronie przeciwpożarowej, jednak do końca naszej kontroli projekty te nie zostały ukończone.

Nabór do służb

W 2012 r. nasz nowo powstały departament przeprowadził kontrolę dotyczącą naboru, postępowania kwalifikacyjnego i szkolenia nowych funkcjonariuszy ABW, CBA, Policji i Straży Granicznej[8]. Była to pierwsza, niełatwa kontrola realizacji zadań przez służby specjalne.

W ocenie Izby, system naboru do służby i postępowania kwalifikacyjnego kandy-

[4] Kontrola P/11/074.
[5] Kontrola: *Gromadzenie, przetwarzanie i udostępnianie informacji dotyczących bezpieczeństwa imprez masowych*, nr P/11/186.
[6] Kontrola: *Funkcjonowanie numeru alarmowego na terenie Polski*, nr P/09/061.
[7] Ustawa z 5.12.2008 o zmianie ustawy o ochronie przeciwpożarowej oraz niektórych innych ustaw (Dz.U. z 2009 r. nr 11 poz. 59).
[8] Kontrola: *Nabór, postępowanie kwalifikacyjne i szkolenie nowo przyjętych funkcjonariuszy ABW, CBA, Policji i Straży Granicznej*, nr P/12/093.

datów oraz służby przygotowawczej nowo przyjętych funkcjonariuszy, zapewniał prawidłową realizację zadań nałożonych przepisami prawa. Wprowadzone zasady i procedury umożliwiały efektywne pozyskiwanie najlepszych kandydatów, którzy po właściwym przeszkoleniu i adaptacji zawodowej rozpoczynali realizację zadań w ramach służby stałej.

Mimo to, stwierdziliśmy nieprawidłowości, między innymi w Agencji Bezpieczeństwa Wewnętrznego. Dotyczyły długotrwałości postępowań kwalifikacyjnych; sporządzania końcowych ocen predyspozycji przed zakończeniem postępowania lub ich niezatwierdzania przez kierowników jednostek organizacyjnych ABW prowadzących postępowanie; opóźnień w składaniu ślubowania przez nowych funkcjonariuszy. Stwierdzono również opóźnienia w kierowaniu nowo przyjętych na szkolenie podoficerskie oraz opóźnienia w sporządzaniu wymaganych opinii służbowych.

Ponadto krytycznie oceniliśmy działalność Szefa Centralnego Biura Antykorupcyjnego. Nieprawidłowości były poważne i dotyczyły: przeprowadzania postępowań kwalifikacyjnych niezgodnie z ustawą o CBA i rozporządzeniami wykonawczymi regulującymi nabór i postępowanie kwalifikacyjne kandydatów, w tym ocenę ich zdolności do służby; prowadzenia, wbrew obowiązującym przepisom, badań wariograficznych w stosunku do wszystkich kandydatów objętych pełną procedurą postępowania kwalifikacyjnego; braków w dokumentacji, w tym potwierdzenia złożenia przysięgi; niesporządzania lub nieterminowego sporządzania opinii służbowych; nierzetelnego planowania i nieefektywnej realizacji szkoleń.

Warto jednak podkreślić, że jeszcze w trakcie kontroli szef CBA podjął kompleksowe działania, aby wyeliminować stwierdzone nieprawidłowości.

Szefowie ABW i CBA poddawali badaniom na wykrywaczu kłamstw wszystkich kandydatów do służby, mimo że obowiązujący wówczas stan prawny zobowiązywał ich do określenia jedynie wybranych stanowisk, na które ubiegający się o przyjęcie mogli być zostać przebadani w ten sposób. Nie kwestionując celowości stosowania przedstawionych wyżej rozwiązań, w szczególności mających na celu rzetelną weryfikację kandydatów, stanęliśmy na stanowisku, że objęte kontrolą służby odpowiadające za bezpieczeństwo wewnętrzne państwa, są szczególnie zobowiązane do działania zgodnie z zasadą wyrażoną w art. 7 Konstytucji RP[9], tj. działania organów władzy publicznej wyłącznie na podstawie i w granicach prawa. Dlatego też wszelkie rozwiązania ograniczające prawa i wolności obywatelskie powinny być, zgodnie z art. 31 ust. 3 i art. 87 ust. 1 Konstytucji, wprowadzane w drodze aktów powszechnie obowiązujących, a możliwość ich stosowania ściśle ograniczona do wypadków wskazanych w tych przepisach.

Działania NIK przyniosły założony skutek, bowiem wszystkie wnioski pokontrolne zostały zrealizowane.

[9] Ustawa Konstytucja Rzeczypospolitej Polskiej z 2.4.1997, Dz.U. nr 78 poz. 483, ze zm.

Problem narkomanii w szkołach

Podejmowaliśmy również tematy trudne, ale społecznie bardzo ważne, umożliwiające podejmowanie działań zapobiegających dramatom wielu rodzin. Bez wątpienia należy do nich kontrola profilaktyki narkomanii w szkołach.

We wszystkich kontrolowanych przez Izbę placówkach prowadzono dla uczniów zajęcia z zakresu profilaktyki narkomanii, jednak ich jakość pozostawała na niskim poziomie i nie zapewniała skuteczności. Przyczyną niesięgania przez szkoły po programy profilaktyczne o potwierdzonej skuteczności było głównie błędne przekonanie dyrektorów szkół o niewystępowaniu problemu narkotyków w ich szkołach. Tymczasem w badaniach ankietowych przeprowadzonych przez NIK w trakcie kontroli, ponad 31% badanych uczniów przyznało, że na terenie swojej szkoły było świadkiem używania narkotyków lub słyszało o tym od koleżanek/kolegów. Na pytanie dotyczące sprzedaży narkotyków twierdząco odpowiedziało 17% uczniów. Problem zażywania przez nich narkotyków dostrzegało też ponad 28% ankietowanych nauczycieli, a 22% przyznawało, że nie ma na ten temat wiedzy. Ustalono ponadto, że na terenie właściwości ośmiu kontrolowanych komend miejskich Policji w okresie 2010–2012 (I półrocze) było 4638 osób posiadających środki odurzające lub substancje psychotropowe, wśród których 12% stanowili nieletni. Posiadanie znacznej ilości takich środków lub substancji stwierdzono w przypadku 323 osób, wśród których 0,6% stanowili nieletni.

Tylko w 10 spośród 32 kontrolowanych szkół wdrażano programy profilaktyki uniwersalnej (lub ich elementy), których skuteczność została potwierdzona w badaniach naukowych[10]. Dotyczyło to łącznie tylko sześciu takich programów, z których cztery były przeznaczone dla uczniów, a dwa dla rodziców i nauczycieli. Takich programów nie realizowano w żadnej z ośmiu szkół kształcenia ponadgimnazjalnego, choć wskaźniki zażywania narkotyków na tym etapie edukacji były najwyższe. W większości szkół profilaktyka narkomanii ograniczała się do poruszania tego zagadnienia przez nauczycieli w trakcie zajęć dydaktycznych i godzin wychowawczych, oglądania filmów i spektakli profilaktycznych czy organizacji konkursów plastycznych i literackich, a więc działań o nieznanej lub niskiej skuteczności. System Rekomendacji Programów Profilaktycznych i Promocji Zdrowia Psychicznego, mający na celu szersze upowszechnianie wiedzy o dobrych praktykach, opracowano dopiero pod koniec 2010 r. Pierwsze rekomendowane programy pojawiły się dopiero w 2012 r. (do 30 września były cztery). Bank Programów Profilaktycznych ORE zawierał natomiast jedynie 12 programów do realizacji w klasach[11], z czego

[10] W kontroli przyjęto, że działaniami profilaktycznymi o potwierdzonej skuteczności są programy profilaktyczne rekomendowane w ramach systemu Rekomendacji, umieszczone w europejskiej bazie EDDRA oraz w Banku Programów Profilaktycznych ORE.

[11] Według stanu od maja 2011 r. do zakończenia kontroli.

tylko trzy były przystosowane do zastosowania w szkołach ponadgimnazjalnych[12].

Aż dwanaście spośród 32 skontrolowanych szkół zdiagnozowało podwyższone ryzyko sięgania po narkotyki przez uczniów. Mimo to, nie zintensyfikowano tam działań profilaktycznych lub nie wykazano szczególnej dbałości o ich jakość i skuteczność.

W siedmiu spośród wymienionych 12 szkół nie zaplanowano działań z zakresu profilaktyki selektywnej, tj. ukierunkowanej na zagrożonych uczniów, a w 10 – działań o potwierdzonej skuteczności wpływu na zachowania dzieci i młodzieży. Ponadto w czterech spośród nich nauczyciele nie przeszli w okresie objętym kontrolą żadnych szkoleń dotyczących zagrożenia narkomanią lub metodyki prowadzenia działań profilaktycznych.

Główny ciężar realizacji działań profilaktycznych w szkołach spoczywał na nauczycielach oraz pedagogach i psychologach szkolnych, jednak nauczyciele z 12 kontrolowanych szkół oraz pedagodzy i psycholodzy szkolni z 9 placówek nie uczestniczyli w badanym okresie w żadnych szkoleniach z tego obszaru. Dyrektorzy wyjaśniali to przede wszystkim brakiem zapotrzebowania ze strony samej kadry pedagogicznej, chociaż to na dyrektorach – zgodnie z § 3 rozporządzenia MENiS w sprawie działalności wychowawczej i zapobiegawczej – spoczywała odpowiedzialność za przygotowanie nauczycieli do realizacji działań wychowawczych i zapobiegawczych.

Działania profilaktyczne w szkołach prowadziły także podmioty zewnętrzne, głównie Policja, a także straże miejskie i Prokuratura, lecz ich działalność ograniczała się do informowania o odpowiedzialności prawnej nieletnich za używanie, posiadanie i dystrybucję narkotyków.

W okresie objętym kontrolą w dziewięciu spośród 32 skontrolowanych szkół wystąpiło łącznie 17 incydentów związanych z narkotykami, w związku z którymi szkoły podjęły działania interwencyjne. Polegały one głównie na zawiadomieniu rodziców lub opiekunów oraz wezwaniu Policji i były zgodne z przepisami prawa oraz przyjętymi w szkołach procedurami postępowania w sytuacjach szczególnych zagrożeń. Na podkreślenie zasługuje, że we wszystkich przypadkach uczniów tych objęto dodatkowymi działaniami profilaktycznymi lub udzielano im i ich rodzicom/opiekunom wzmożonej pomocy psychologiczno-pedagogicznej.

Wyniki naszej kontroli odbiły się szerokim echem, uświadomiły bowiem obywatelom rozdźwięk pomiędzy brakiem działań dyrektorów niemal wszystkich skontrolowanych szkół, a istniejącym problemem narkomanii w kierowanych przez nich placówkach.

Informatyka w Policji

W działalności departamentu, wybierając tematy kontroli, dużą wagę przykładaliśmy do wykorzystywania nowych technologii. Dlatego poddaliśmy kontroli budowę i eksploatację dwóch kluczowych

[12] „Spójrz inaczej", „Tak czy nie" oraz „Trzeci elementarz, czyli program siedmiu kroków".

dla Policji systemów teleinformatycznych: Systemu Wspomagania Dowodzenia (SWD) i E-posterunek[13].

Od 1 stycznia 2013 r. system SWD został wdrożony i jest wykorzystywany, w szczególności przez funkcjonariuszy służby dyżurnej, w jednostkach Policji na terenie całego kraju. Komenda Główna Policji (KGP) nie była jednak należycie przygotowana do realizacji tego przedsięwzięcia teleinformatycznego oraz do wykorzystania dofinansowania ze środków UE przyznanego na rozbudowę SWD. W całym okresie objętym kontrolą nie były prowadzone rzetelne prace planistyczne, pozwalające na określenie jednolitej i aktualizowanej na bieżąco koncepcji, zawierającej w szczególności cele projektu, harmonogram budowy systemu, całościowy budżet oraz koszty utrzymania SWD. KGP nie dysponowała wiedzą na temat zasad kwalifikowalności wydatków podlegających dofinansowaniu ze środków UE oraz nie prowadziła rzetelnych analiz, mających na celu określenie faktycznych możliwości wykorzystania przyznanego dofinansowania. W naszej ocenie, nierzetelna i nieskuteczna była również współpraca między KGP a Centrum Projektów Informatycznych (CPI). W wyniku stwierdzonych nieprawidłowości wykorzystano tylko 1,8 mln zł z pierwotnego dofinansowania ze środków UE w kwocie 150 mln zł; wystąpiło też ryzyko niewykorzystania większości zarezerwowanych na ten cel środków.

Zdecydowanie negatywnie oceniliśmy natomiast budowę systemu e-posterunek. W całym okresie objętym kontrolą, tj. zarówno na etapie przygotowania przedsięwzięcia, jak i w trakcie jego realizacji, w KGP nie opracowano formalnych dokumentów planistycznych projektu e-posterunek, wymaganych na podstawie obowiązujących w Policji wewnętrznych przepisów dotyczących prowadzenia przedsięwzięcia teleinformatycznego.

Planowanie projektu e-posterunek prowadzono bez przygotowania i bez dochowania należytej staranności. W całym okresie realizacji tego przedsięwzięcia nie zostały stworzone rzetelne i aktualizowane na bieżąco dokumenty dotyczące kluczowych obszarów podlegających planowaniu w związku z prowadzonym przedsięwzięciem teleinformatycznym, takie jak: dokument określający cele budowy aplikacji, harmonogram wykonania oraz plan finansowy projektu. Nie zostały określone wymagania odnośnie do parametrów sprzętu przeznaczonego do obsługi e-posterunku, ani nie oszacowano potrzeb jednostek organizacyjnych Policji związanych z wyposażeniem w sprzęt informatyczny do obsługi tej aplikacji. W KGP nie określono kosztów utrzymania nowo budowanego systemu teleinformatycznego oraz nie przeprowadzono analizy uwarunkowań prawnych wdrożenia aplikacji e-posterunek do praktyki policyjnej.

W wypadku tego projektu, odwrócono kolejność działań prawidłową dla przedsięwzięć teleinformatycznych, tj. najpierw zamówiono i odebrano aplikację teleinformatyczną, którą przekazano do użytkowania

[13] Kontrola: *Planowanie i realizacja wybranych projektów teleinformatycznych, mających na celu usprawnienie funkcjonowania jednostek organizacyjnych Policji*, nr P/12/096.

funkcjonariuszom Policji, a dopiero w drugiej kolejności rozpoczęto analizy dotyczące warunków prawnych, finansowych i technicznych wdrożenia tego narzędzia do praktyki policyjnej, co NIK oceniła negatywnie.

W całym okresie objętym kontrolą między komórkami organizacyjnymi KGP nie została wypracowana jednolita koncepcja realizacji projektu e-posterunek. Przedsięwzięcie było prowadzone w warunkach konfliktu między Biurem Łączności i Informatyki (BŁiI), KGP (odpowiadającym za realizację projektów teleinformatycznych) a Biurem Kryminalnym (BK) KGP (reprezentującym głównego użytkownika końcowego budowanej aplikacji – policjantów służby dochodzeniowo-śledczej).

Decyzje dotyczące rozbudowy e-posterunku były podejmowane jednostronnie przez kierownictwo BŁiI KGP oraz nadzorującego tę komórkę organizacyjną zastępcę Komendanta Głównego Policji, bez przeprowadzenia rzetelnych konsultacji z właściwymi komórkami merytorycznymi Komendy Głównej oraz mimo braku zainteresowania nowymi funkcjonalnościami ze strony użytkowników, dla których system był tworzony. KGP nie podjął działań nadzorczych w celu rozstrzygnięcia konfliktu i nie wydał wytycznych wiążących wszystkich uczestników przedsięwzięcia, dotyczących zasadności, formy i zakresu dalszej realizacji projektu.

Kierownictwo BŁiI KGP nie sprawowało nadzoru nad wykonaniem umowy i odbiorem aplikacji e-posterunek. Skutkowało to m.in. odebraniem przez CPI i przekazaniem funkcjonariuszom Policji produktu niespełniającego oczekiwań użytkowników i niezapewniającego skutecznej obsługi zadań służbowych.

W jednostkach organizacyjnych Policji objętych kontrolą NIK wykorzystywano poszczególne funkcjonalności e-posterunku w ograniczonym zakresie, przy czym w czterech z 12 zbadanych jednostek w ogóle nie używano tego systemu. Część zakupionych funkcjonalności tej aplikacji nie została w ogóle udostępniona przez KGP funkcjonariuszom Policji i obywatelom. Przekazany sprzęt informatyczny przeznaczony do obsługi e-posterunku w większości przypadków nie był wykorzystywany do pracy z tą aplikacją. Stwierdzono również przypadki niegospodarnego zarządzania otrzymanymi urządzeniami. Komórki organizacyjne KGP odpowiedzialne za wdrożenie e-posterunku nie prowadziły rzetelnych i systematycznych działań związanych z monitorowaniem stanu wykorzystania aplikacji przez terenowe jednostki organizacyjne Policji. W związku z powyższym, decyzje dotyczące rozbudowy systemu i jego dalszego rozwoju wizji były podejmowane bez gruntownej wiedzy na temat użyteczności tego narzędzia i problemów z jego wdrażaniem

Uruchomienie aplikacji e-posterunek w terenowych jednostkach organizacyjnych Policji nastąpiło nielegalnie, w sytuacji niewypełnienia przez Komendanta Głównego Policji obowiązków administratora danych wymienionych w art. 36 ustawy o ochronie danych osobowych, dotyczących w szczególności opracowania polityki bezpieczeństwa i instrukcji zarządzania systemem informatycznym. Stworzyło to zagrożenie dla integralności, poufności i rozliczalności przetwarzanych

w tej aplikacji danych osobowych obywateli i policjantów. Działania, mające na celu wyeliminowanie przypadków naruszenia prawa w obszarze przetwarzania danych osobowych, zostały podjęte przez Komendanta Głównego Policji dopiero po otrzymaniu od kontrolerów NIK informacji o wspomnianych nieprawidłowościach.

Ustalono, że pomimo nieuruchomienia znacznej części zakupionych funkcjonalności oraz niedysponowania rzetelną wiedzą na temat stanu wdrożenia tego narzędzia w jednostkach Policji, w KGP planowano dalszy rozwój tej aplikacji przez budowę centralnej bazy danych postępowań i zdarzeń drogowych gromadzonych w e-posterunku. Koszty dalszych prac rozwojowych oszacowano na kwotę ok. 15 mln zł. NIK zwróciła uwagę na konieczność wstrzymania dalszych wydatków na rozwój e-posterunku do momentu podjęcia przez kierownictwo KGP wiążących decyzji dotyczących wykorzystania tego narzędzia w Policji oraz usunięcia nieprawidłowości w realizacji przedsięwzięcia.

Można powiedzieć, że w wyniku kontroli uratowaliśmy 15 mln zł, ponieważ decyzją Komendanta Głównego Policji aplikacja e-posterunek, na której wytworzenie oraz wyposażenie w sprzęt dostępowy wydano 19 371,9 tys. zł, nie została wdrożona do praktyki policyjnej. Ustalenia kontroli odebrano – nie tylko w Policji – jako instruktaż, jak nie budować systemów teleinformatycznych.

Cyberbezpieczeństwo

Niezwykle ważne jest w każdym państwie zapewnienie bezpieczeństwa cyberprzestrzeni. Wyniki kontroli opublikowanej w 2015 roku[14] nie pozostawiały wątpliwości, że w Polsce nie jest ona właściwie chroniona.

Stwierdziliśmy, że 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 problemy. Kluczowym czynnikiem paraliżującym aktywność państwa był brak jednego ośrodka decyzyjnego, koordynującego działania innych instytucji publicznych. Nie zidentyfikowano podstawowych zagrożeń dla krajowej infrastruktury teleinformatycznej oraz nie wypracowano narodowej strategii ochrony cyberprzestrzeni, stanowiącej podstawę do działań podnoszących bezpieczeństwo teleinformatyczne. Nie określono też struktury i ram prawnych krajowego systemu ochrony cyberprzestrzeni, nie zdefiniowano obowiązków i uprawnień jego uczestników oraz nie przydzielono zasobów niezbędnych do skutecznej realizacji zadań. A co najważniejsze, nie przygotowano procedur reagowania w sytuacjach kryzysowych.

W naszej ocenie, istotnym czynnikiem było niewystarczające zaangażowanie kierownictwa administracji rządowej, w tym Prezesa Rady Ministrów, w rozstrzyganie kwestii spornych między poszczególnymi urzędami, czy też zapewnienie

[14] Kontrola: *Realizacja przez podmioty państwowe zadań w zakresie ochrony cyberprzestrzeni Rzeczypospolitej Polskiej*, nr P/14/043.

współdziałania organów i instytucji związanych z bezpieczeństwem teleinformatycznym państwa.

Jako działania pozytywne wykazaliśmy przede wszystkim:

- powołanie i utrzymywanie na wysokim poziomie zespołów ds. bezpieczeństwa informatycznego (CERT) przez takie instytucje, jak Naukowa Akademicka Sieć Komputerowa (NASK), Agencja Bezpieczeństwa Wewnętrznego (ABW) oraz Ministerstwo Obrony Narodowej;
- utworzenie przez Ministra Obrony Narodowej systemu reagowania na incydenty komputerowe w resorcie obrony oraz wyspecjalizowanej jednostki – Narodowego Centrum Kryptologii;
- upowszechnianie przez Rządowe Centrum Bezpieczeństwa 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.

Ponadto zwróciliśmy uwagę, że poszczególne kontrolowane podmioty posiadały własne, odrębne procedury zapobiegania zagrożeniom w cyberprzestrzeni. Ale suma tych rozwiązań nie tworzyła jednego spójnego systemu.

Kontrola NIK wykazała, że Minister Administracji i Cyfryzacji, któremu bezpośrednio przypisano obowiązki związane z ochroną cyberprzestrzeni, nie realizował należących do niego zadań w zakresie inicjowania i koordynowania działań innych podmiotów w dziedzinie bezpieczeństwa teleinformatycznego państwa. Nie dysponował zasobami pozwalającymi na rzeczywistą realizację zadań dotyczących zarządzania krajowym systemem ochrony cyberprzestrzeni oraz nie miał uprawnień do oddziaływania na inne instytucje, które odmawiały współpracy lub nierzetelnie i nieterminowo wywiązywały się z przypisanych im obowiązków.

Natomiast 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, ale nawet w tym zakresie były prowadzone w sposób nierzetelny.

Stwierdziliśmy również, że obowiązujące wówczas przepisy Prawa telekomunikacyjnego były wadliwie sformułowane i nie mogły być w praktyce wykorzystywane do realizacji zadań związanych z bezpieczeństwem IT. Stało się to przyczyną zaniechania wykonywania obowiązków przez Prezesa Urzędu Komunikacji Elektronicznej, dotyczących zwłaszcza pozyskiwania informacji o incydentach występujących w cyberprzestrzeni oraz informowania obywateli o zagrożeniach związanych z korzystaniem z Internetu.

Koordynowany przez Rządowe Centrum Bezpieczeństwa system zarządzania kryzysowego nie był komplementarny i spójny z działaniami w zakresie bezpieczeństwa teleinformatycznego oraz w niewystarczającym stopniu uwzględniał nowe zagrożenia dla infrastruktury krytycznej państwa, jakimi są te występujące w cyberprzestrzeni.

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 kompleksowego systemu reagowania na zagrożenia i incydenty w cyberprzestrzeni.

Minister Obrony Narodowej realizował zadania dotyczące budowy resortowego systemu reagowania na incydenty komputerowe oraz uczestniczył w budowie krajowego systemu ochrony cyberprzestrzeni.

Kierownictwo ABW wykonywało 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 jednak istotnym ograniczeniom, wynikającym zwłaszcza z niewystarczających zasobów i braku formalnego umocowania wspomnianego Zespołu.

Kierownictwo Naukowej i Akademickiej Sieci Komputerowej podejmowało liczne działania, które oceniliśmy jako dobre praktyki w zakresie ochrony cyberprzestrzeni. Dotyczyły one w szczególności powołania i utrzymywania zespołu CERT Polska.

Stwierdziliśmy ponadto, że już od 2008 r. prowadzone były prace nad narodową strategią ochrony cyberprzestrzeni. Kolejne wersje tego dokumentu nie były jednak zatwierdzane ze względu na ich nierzetelne przygotowanie i sprzeczne interesy różnych instytucji, zaangażowanych w przygotowywanie strategii.

W czerwcu 2013 r. Rada Ministrów przyjęła „Politykę ochrony cyberprzestrzeni Rzeczypospolitej Polskiej" – dokument będący wynikiem źle rozumianego kompromisu, nieprecyzyjny i obarczony licznymi błędami merytorycznymi. Nielicznych zadań wynikających bezpośrednio z „Polityki" nie realizowała większość skontrolowanych przez NIK podmiotów, co pozwala stwierdzić, że praktyczne zastosowanie strategii w celu poprawy bezpieczeństwa teleinformatycznego państwa było raczej symboliczne.

Nie były opracowane także założenia systemu finansowania działań związanych z ochroną cyberprzestrzeni RP. Nie przydzielono żadnych dodatkowych środków na ich realizację, co w ocenie NIK sparaliżowało działania podmiotów państwowych. Zasoby poszczególnych jednostek objętych kontrolą były bowiem nieadekwatne w stosunku do przypisanych im obowiązków.

Nie prowadzono żadnych prac legislacyjnych, które miałyby na celu unormowanie zagadnień związanych z bezpieczeństwem teleinformatycznym państwa. Nie przeprowadzono inwentaryzacji przepisów rozproszonych w różnych aktach prawnych, ani nie zdefiniowano pożądanych kierunków zmian legislacyjnych. Nie przygotowano nawet założeń aktu normatywnego określającego strukturę krajowego systemu ochrony cyberprzestrzeni i jego uczestników.

W Polsce wciąż nie funkcjonował spójny krajowy system reagowania na incydenty komputerowe. Czynności z tym związane były realizowane przez funkcjonujące niezależnie od siebie państwowe i prywatne zespoły CERT, zajmujące się własnymi obszarami oddziaływania. Kierownictwo administracji państwowej nie podejmowało działań służących wypracowaniu założeń

pożądanej struktury zespołów reagowania, ustanowieniu kanałów wymiany informacji oraz powołaniu CERT narodowego, koordynującego działania wielu podmiotów i odpowiadającego za współpracę międzynarodową.

Minister Administracji i Cyfryzacji, który zgodnie z zapisami strategii odpowiada za koordynację krajowego systemu reagowania na incydenty komputerowe, nie realizował żadnych zadań w tym zakresie.

Administracja państwowa nie dysponowała 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.

Tworzone w Polsce plany kryzysowe, w tym Krajowy Plan Zarządzania Kryzysowego, odnosiły się wyłącznie do zdarzeń konwencjonalnych, 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 do opracowania procedur obowiązujących w sytuacjach kryzysowych związanych z cyberprzestrzenią, a kierownictwo odpowiedzialnych podmiotów państwowych nie dostrzegało potrzeby podjęcia stosownych działań.

Dostrzegliśmy jednak wysiłki podejmowane przez ABW (we współpracy z NASK) w celu realizacji projektu dotyczącego wytworzenia, utrzymywania i rozbudowy systemu wczesnego ostrzegania – ARAKIS.GOV. W ramach tego przedsięwzięcia w kilkudziesięciu instytucjach publicznych zainstalowano sondy systemu, dzięki którym uzyskiwano informacje o zagrożeniach w Internecie. Jednak ze względu na braki finansowe, dobrowolność udziału w projekcie oraz instalowanie sond wyłącznie w podmiotach publicznych, zasięg oddziaływania systemu oraz pozyskiwanych za jego pomocą danych miał ograniczony zakres.

Administracja publiczna nie wypracowała zintegrowanego i systemowego wspierania przez państwo badań w obszarze ochrony cyberprzestrzeni oraz możliwości praktycznego zastosowania ich wyników do poprawy bezpieczeństwa teleinformatycznego.

W naszej ocenie istniała konieczność bezzwłocznego podjęcia skoordynowanych, systemowych działań, prowadzących do wdrożenia 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 było bezpośrednie zaangażowanie w realizację zadań Rady Ministrów i Prezesa Rady Ministrów. Kolejnymi warunkami efektywnej ochrony cyberprzestrzeni było wdrożenie mechanizmów współpracy podmiotów prywatnych i państwowych oraz zapewnienie odpowiedniego finansowania działań związanych z bezpieczeństwem IT. Realizując wniosek pokontrolny NIK, Prezes Rady Ministrów z rezerwy celowej przekazał do ABW kilkanaście milionów zł na sfinansowanie koniecznych przedsięwzięć dotyczących cyberbezpieczeństwa.

W czerwcu 2018 r. NIK wszczęła kontrolę[15], której głównym celem jest sprawdzenie, czy właściwe organy państwa prawidłowo i skutecznie zarządzają ryzykiem związanym z zagrożeniami występującymi w cyberprzestrzeni RP. Objęto nią 8 tych samych podmiotów państwowych, którym przypisano kluczowe zadania związane z bezpieczeństwem teleinformatycznym państwa[16]. Przedstawienie wyników kontroli zaplanowano na koniec I kwartału 2019 r.

Na podstawie wstępnych wyników kontroli można stwierdzić, że zmieniło się podejście do spraw związanych z cyberprzestrzenią. Istnieje świadomość niebezpieczeństw oraz wynikających z tego faktu nowych zadań administracji państwowej. Zaczęły też obowiązywać: dyrektywa NIS, Krajowe Ramy Polityki Cyberbezpieczeństwa RP na lata 2017–2022 oraz ustawa z 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa[17]. Czy organy administracji publicznej definiują cyberbezpieczeństwo jako proces wymagający nakładów finansowych i czy konsekwencją tego podejścia są rzetelne i skuteczne działania kształtujące bezpieczną przestrzeń teleinformatyczną RP, tak jak postulowała to NIK w 2015 r., okaże się po zakończeniu kontroli.

Nadzór nad służbami specjalnymi

Oceniając wpływ rezultatów kontroli na poprawę bezpieczeństwa wewnętrznego kraju, nie sposób pominąć dwóch dotyczących służb specjalnych. Pierwsza: „Organizacja służb specjalnych oraz nadzór nad nimi”[18], została przeprowadzona przez ówczesny Departament Obrony Narodowej i Bezpieczeństwa Wewnętrznego od 17 czerwca 2004 r. do 17 maja 2005 r. i objęła okres od 29 czerwca 2002 r. do 30 czerwca 2004 r. Była to pierwsza kontrola dotycząca organizacji i merytorycznego funkcjonowania służb specjalnych, a jej przeprowadzenie wiązało się z poważnymi zmianami legislacyjnymi.

Celem kontroli było zbadanie i ocena organizacji i realizacji zadań przez Agencję Bezpieczeństwa Wewnętrznego, Agencję Wywiadu (AW) i Wojskowe Służby Informacyjne (WSI), zwane dalej „służbami specjalnymi”. Ponadto, przeprowadzenie kontroli pozwoliło na ocenę funkcjonowania systemów kierowania i nadzoru nad nimi oraz działanie ustawowych środków odwoławczych. W tym czasie, 29 czerwca 2002 r., weszła bowiem w życie ustawa o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu[19], na mocy której utworzono obie służby i równocześnie zlikwidowano Urząd Ochrony Państwa. Wojskowe Służby

[15] Kontrola: *Bezpieczeństwo teleinformatyczne RP*, nr P/18/036.
[16] To jest: Ministerstwo Cyfryzacji, Agencję Bezpieczeństwa Wewnętrznego, Ministerstwo Obrony Narodowej, Ministerstwo Spraw Wewnętrznych i Administracji, Naukową i Akademicką Sieć Komputerową, Urząd Komunikacji Elektronicznej, Rządowe Centrum Bezpieczeństwa oraz Komendę Główną Policji.
[17] Ustawa weszła w życie 28.8.2018.
[18] Kontrola: *Organizacja służb specjalnych oraz nadzór nad nimi*, nr I/04/001.
[19] Ustawa z 24.5.2002 o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu (tekst pierwotny opublikowany 14.6.2002 w Dz.U. nr 74 poz. 676. Obowiązujący obecnie tekst jednolity opublikowany w Dz.U. z 2017 r. poz. 1920, ze zm.).

Informacyjne zaczęły zaś funkcjonować 23 sierpnia 2003 r., kiedy weszła w życie ustawa, powołująca tę strukturę[20].

Ustawa o ABW i AW zobowiązała Radę Ministrów lub Prezesa Rady Ministrów do wydania 49 rozporządzeń i 5 zarządzeń regulujących organizację i funkcjonowanie ABW oraz 44 rozporządzeń i 3 zarządzeń dotyczących Agencji Wywiadu. Do dnia zakończenia kontroli Prezes Rady Ministrów nie wydał 5 rozporządzeń dotyczących ABW oraz 4 rozporządzeń odnoszących się do AW. Projekty aktów wykonawczych były opracowywane i poddawane procedurze legislacyjnej samodzielnie przez szefów Agencji. W ocenie Najwyższej Izby Kontroli nie dołożyli oni należytej staranności, aby sprawnie je opracować, co było zasadniczą przyczyną długotrwałego tworzenia podstaw prawnych funkcjonowania tych organów. Pomimo upływu dwóch i pół roku od wejścia w życie ustawy, nie doprowadzono do stworzenia pełnego systemu prawnego określonego ustawą, dającego podstawy funkcjonowania Agencji. Zdaniem Najwyższej Izby Kontroli świadczyło to o niedostatecznym nadzorze Prezesa Rady Ministrów nad działalnością Agencji w tym zakresie. Uchwalenie nowej ustawy, regulującej zagadnienia dotyczące ochrony bezpieczeństwa zewnętrznego i wewnętrznego państwa oraz utworzenie nowych struktur organizacyjnych do realizacji zadań przewidzianych w ustawie, dowodziło że dotychczasowe regulacje nie w pełni przystawały do potrzeb.

Ustawa o WSI zobowiązała Radę Ministrów, Prezesa Rady Ministrów i Ministra Obrony Narodowej do wydania 14 rozporządzeń oraz 15 zarządzeń regulujących organizację i funkcjonowanie tych służb. W terminie ustalonym w ustawie o WSI weszły w życie wszystkie rozporządzenia. Natomiast z 15 zarządzeń, wydano tylko 5. Prezes Rady Ministrów wydał 3 na 5 wymaganych, a Minister Obrony Narodowej 2 z 10. Niedotrzymanie terminu ustanowienia wszystkich przepisów prawnych dotyczących funkcjonowania WSI było w ocenie Najwyższej Izby Kontroli działaniem nielegalnym. Niewydanie w terminie zarządzeń wykonawczych, przy jednoczesnej utracie mocy przez wszystkie poprzednio obowiązujące w tej materii regulacje prawne, spowodowało sytuację podejmowania przez WSI działań niemających oparcia w przepisach prawa. Zarządzenia nie zostały wydane w wyznaczonym terminie, ponieważ Ministerstwo Obrony Narodowej prowadziło prace legislacyjne dopiero w 2004 r., co NIK oceniła jako nierzetelne.

Przekazywanie przez służby specjalne Instytutowi Pamięci Narodowej dokumentów, zbiorów danych, rejestrów i kartotek, a także akt funkcjonariuszy, wytworzonych lub gromadzonych do 6 maja 1990 r., przebiegało w terminach niezgodnych z prawem. Do czasu zakończenia kontroli

[20] Ustawa z 9.7.2003 o Wojskowych Służbach Informacyjnych. Tekst pierwotny opublikowano 8.8.2003 w Dz.U. nr 139 poz. 1326. Ustawa została uchylona 30.9.2006 na mocy art. 3 ustawy z 9.6.2006. Przepisy wprowadzające ustawę o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego oraz ustawę o służbie funkcjonariuszy Służby Kontrwywiadu Wojskowego oraz Służby Wywiadu Wojskowego (Dz.U. nr 104 poz. 711).

proces ten był kontynuowany w Agencji Wywiadu i Wojskowych Służbach Informacyjnych, a kolejne terminy wyznaczane przez Prezesa IPN nie były dotrzymywane; NIK uznała to za nierzetelne. Ponadto, Agencja Wywiadu weszła w posiadanie części zasobów archiwalnych byłego Urzędu Ochrony Państwa w sposób naruszający obowiązujące przepisy.

Nadzór Prezesa Rady Ministrów oraz Ministra Obrony Narodowej nad służbami specjalnymi był niewystarczający. Organy kontrolne Kancelarii Prezesa Rady Ministrów (KPRM) oraz Ministra nie prowadziły kontroli działalności merytorycznej i funkcjonowania tych służb. Sprawowanie nadzoru, którego zasadniczym celem jest usuwanie nieprawidłowości w realizacji zadań, bez dopływu informacji dostarczanych w wyniku prowadzonych kontroli, nie dawało możliwości pełnego monitorowania nadzorowanych organów. Przekazywanie przez Prezesa Rady Ministrów szefom Agencji części istotnych zadań do realizacji w formie ustnej, w ocenie Najwyższej Izby Kontroli było nierzetelnym wykonywaniem kompetencji organu państwa. Nie dawało to możliwości ustalenia, kto i kiedy podejmował konkretne rozstrzygnięcia oraz jaki był przebieg realizacji tych rozstrzygnięć. Zdaniem NIK zaniechanie kontroli instytucjonalnej służb specjalnych utrudniało sprawowanie skutecznego nadzoru nad wykonywaniem ich ustawowych zadań.

Kolegium do spraw Służb Specjalnych, jako organ opiniodawczo-doradczy Rady Ministrów w sprawach ich programowania, nadzorowania i koordynowania działalności, nie w pełni realizowało zadania określone w ustawie o ABW i AW oraz planach pracy Kolegium, w tym obowiązku opiniowania dokumentów planistycznych i sprawozdawczych z działalności służb. Przebieg posiedzeń Kolegium był dokumentowany w protokołach, z uwzględnieniem podejmowanych rozstrzygnięć i wygłaszanych opinii, jednak pomimo obowiązku prawnego, sekretarz Kolegium nie prowadził rejestru ocen lub opinii Kolegium i decyzji przewodniczącego Kolegium oraz harmonogramu ich realizacji. W ocenie NIK stanowiło to istotne utrudnienie w sprawowaniu nadzoru nad realizacją tych decyzji.

Krytyczna ocena NIK dotycząca nieudostępnienia kontrolerom części dokumentów zawierających przepisy regulujące prowadzenie czynności operacyjno-rozpoznawczych była przedmiotem zastrzeżeń zgłoszonych przez obu szefów Agencji do Kolegium NIK. Zastrzeżenia te zostały oddalone przez Kolegium Najwyższej Izby Kontroli.

Biorąc pod uwagę stwierdzone nieprawidłowości i uchybienia, NIK uznała za niezbędną m.in. realizację następujących wniosków:

- objęcie skutecznym nadzorem Prezesa Rady Ministrów działalności Agencji Bezpieczeństwa Wewnętrznego i Agencji Wywiadu, między innymi przez określanie zadań i rozliczanie z ich wykonania, zachowując przy tym formę pisemną oraz zlecanie przeprowadzania kontroli działalności merytorycznej tych służb podległym sobie organom kontrolnym;
- podjęcie przez Prezesa Rady Ministrów działań, które spowodują przedkładanie przez szefów ABW i AW wszystkich dokumentów i materiałów niezbędnych dla potrzeb kontroli NIK;

• prowadzenie przez sekretarza Kolegium do spraw Służb Specjalnych rejestru ocen lub opinii Kolegium, a także decyzji Prezesa Rady Ministrów wraz z harmonogramem ich realizacji.

W 2014 roku NIK przesłała do najważniejszych osób w państwie, w trybie niejawnym, informacje z kolejnej kontroli dotyczącej nadzoru nad służbami specjalnymi, przeprowadzonej przez Departament Porządku i Bezpieczeństwa Wewnętrznego NIK[21]. Prezes Izby – ze względu na wagę ustaleń – podjął jednak decyzję o upublicznieniu najważniejszych wyników tej kontroli.

Rezultaty kolejnej kontroli służb potwierdziły wcześniejsze ustalenia. Obowiązujące przepisy nadal ograniczały możliwość sprawowania skutecznego nadzoru nad służbami specjalnymi przez Prezesa Rady Ministrów. Premier pozbawiony był m.in.: pełnej wiedzy na temat procedur wewnętrznych obowiązujących w służbach specjalnych i kontroli poprawności działań operacyjno-rozpoznawczych w konkretnych, zakończonych sprawach. W istocie więc ustawodawca zobowiązał premiera do nadzoru nad służbami specjalnymi, dając mu ograniczone możliwości weryfikowania przekazywanych przez nie informacji. Taki stan powodował, że w wielu obszarach służby specjalne, pozbawione zewnętrznego cywilnego nadzoru, kontrolowały same siebie.

Funkcję organu opiniodawczo-doradczego w sprawach programowania, nadzorowania i koordynowania działalności służb specjalnych sprawuje Kolegium do spraw Służb Specjalnych. Najwyższa Izba Kontroli stwierdziła, że decyzje podejmowane przez przewodniczącego Kolegium (premiera) w trakcie posiedzeń, w formie poleceń kierowanych do szefów służb specjalnych, organów administracji i członków Kolegium, odnoszące się do obszarów działania tych podmiotów, w znacznym stopniu nie były następnie weryfikowane, bo nie pozwalały na to przepisy. Zdaniem Izby brak systemowego rozwiązania służącego monitorowaniu stopnia realizacji ocen i opinii Kolegium, jak również decyzji Przewodniczącego, pozbawia te organy możliwości bieżącej analizy wykorzystania stanowisk tego gremium oraz ich przydatności do realizacji zadań przez służby specjalne.

Wyniki opisanych wyżej dwóch kontroli przeprowadzonych w ciągu kilkunastu lat przyniosły połowiczny skutek. Najwyższa Izba Kontroli odnotowała podjęte przez Prezesa Rady Ministrów działania legislacyjne mające na celu reformę służb specjalnych z uwzględnieniem konieczności utworzenia niezależnego organu nadzoru nad nimi i tym samym rozwiązania problemów stwierdzonych podczas kontroli. Wykorzystując ustalenia kontroli, Prezes NIK zgłosił uwagi do projektu ustawy o Komisji Kontroli Służb Specjalnych. Wyraził nadzieję, że wnioski NIK pomogą w uregulowaniu tak ważnego obszaru funkcjonowania państwa w sposób umożliwiający kontrolowanie i skuteczne nadzorowanie służb specjalnych przez niezależny

[21] Kontrola: *Realizacja przez organy państwa nadzoru nad służbami prowadzącymi czynności operacyjno-rozpoznawcze*, nr P/13/099.

od nich, zewnętrzny organ. Oczekiwanie to pozostaje niestety nadal aktualne.

Z drugiej zaś strony kontrole te są nie do przecenienia. Wykazały nieprawidłowości o charakterze systemowym oraz uświadomiły nie tylko decydentom, ale również obywatelom, konieczność gruntownych zmian.

Pozyskiwanie bilingów

Brak skutecznego nadzoru nad służbami specjalnymi skonfrontowaliśmy z przestrzeganiem przez te służby oraz sądy, prokuraturę i inne instytucje procedur przy pozyskiwaniu bilingów, o których mowa w art. 180c i d ustawy – Prawo telekomunikacyjne[22].

W ocenie NIK[23], system pozyskiwania i przetwarzania danych zapewniał realizację ustawowych zadań przez kontrolowane podmioty. Wprowadzone zasady i procedury umożliwiały sprawne pozyskiwanie danych w związku z prowadzonymi postępowaniami. Możliwość sięgania po dane telekomunikacyjne mieli jedynie upoważnieni pracownicy i funkcjonariusze, a krąg osób posiadających takie upoważnienie był ściśle określony.

Stwierdzone nieprawidłowości wiązały się m.in. z: przypadkami nieprzestrzegania obowiązujących przepisów, zasad i procedur oraz naruszenia tajemnicy telekomunikacyjnej; pozyskiwaniem danych za pośrednictwem sieci telekomunikacyjnej i systemów teleinformatycznych niespełniających wymagań technicznych i organizacyjnych; żądaniem udostępnienia danych telekomunikacyjnych za okres przekraczający 24 miesiące[24], nieusuwaniem zbędnych danych telekomunikacyjnych; brakiem właściwego nadzoru nad realizowanymi działaniami, w tym w szczególności nad przestrzeganiem przez przedsiębiorców telekomunikacyjnych obowiązków określonych w Prawie telekomunikacyjnym.

W ocenie NIK, obowiązujące przepisy w zakresie pozyskiwania przez uprawnione podmioty danych telekomunikacyjnych nie chronią w stopniu wystarczającym praw i wolności obywatelskich przed nadmierną ingerencją ze strony państwa. Niejednolitość i ogólnikowość przepisów uprawniających do pozyskiwania danych może nasuwać wątpliwości co do współmierności stosowanych ograniczeń praw i wolności obywatelskich w sferze wolności komunikacji z zasadami określonymi w Konstytucji RP.

Należy ponadto zauważyć, że obowiązujący system zbierania informacji dotyczących wykorzystania przez organy państwa danych z bilingów, informacji o lokalizacji oraz innych danych, o których mowa w art. 180c i d ustawy – Prawo telekomunikacyjne nie pozwala na określenie rzeczywistej liczby dokonywanych

[22] Ocena ta została wydana na podstawie badania strony organizacyjno-formalnej uzyskiwania przez uprawnione podmioty danych telekomunikacyjnych. Ze względu na ograniczenia ustawowe kompetencji kontrolnych NIK, przedmiotem kontroli nie mogła być ocena zasadności pozyskiwania danych telekomunikacyjnych.

[23] Kontrola: *Uzyskiwanie i przetwarzanie przez uprawnione podmioty danych z bilingów, informacji o lokalizacji oraz innych danych, o których mowa w art. 180 c i d ustawy Prawo telekomunikacyjne*, nr P/12/191.

[24] Po nowelizacji ustawy Prawo Telekomunikacyjne z 16.11.2012 (Dz.U. z 2012 r. poz. 1445) termin ten od 21.1.2013 uległ skróceniu do 12 miesięcy.

sprawdzeń. Nie istnieją również mechanizmy kontroli o charakterze zewnętrznym, które pozwoliłyby na weryfikację zakresu wykorzystywania danych telekomunikacyjnych przez uprawnione podmioty, a w szczególności zasadności ich pozyskiwania i przetwarzania. Zdefiniowane przez nas problemy są niestety nadal aktualne.

Ruch drogowy

Przed kilkoma laty zajęliśmy się niezwykle istotnym problemem bezpieczeństwa na polskich drogach[25]. Spośród wielu kontroli z tego obszaru, jedną z pierwszych, którą przeprowadził nasz departament była kontrola działań Policji na rzecz bezpieczeństwa obywateli w ruchu drogowym. Jako cel postawiliśmy sobie dokonanie oceny działań podejmowanych przez Policję dla zapewnienia uczestnikom ruchu drogowego szeroko rozumianego bezpieczeństwa oraz wskazanie rozwiązań organizacyjnych i przedsięwzięć wartych spopularyzowania, jako tzw. dobre praktyki.

W wyniku tej kontroli zostały podjęte m.in. następujące działania:

• w 2013 r. zwiększono o 1226 liczbę etatów w pionie ruchu drogowego Policji w stosunku do roku 2012. Na koniec 2013 r. pion ruchu drogowego liczył 9230 etatów, co w rezultacie pozwoliło na wzrost liczby policjantów pełniących służbę na drogach;

• dokonano zmian w organizacji kursów specjalistycznych ruchu drogowego, włączając do realizacji tego zadania Szkoły Policji w Katowicach i Słupsku, co pozwoliło na zwiększenie liczby szkoleń.

W trakcie kontroli stwierdziliśmy m.in., że spośród 7533 policjantów ruchu drogowego zatrudnionych w terenowych jednostkach Policji, tylko 4284 (56,9%) ukończyło kurs specjalistyczny w zakresie ruchu drogowego (RD), wymagany na mocy § 2 i § 4 zarządzenia nr 609 KGP w sprawie pełnienia służby na drogach. Przyczyną tego stanu rzeczy był m.in. niewydolny w stosunku do potrzeb system szkoleniowy Policji. W 2012 r. na kursach RD przeszkolono jedynie 19,6% zgłoszonych funkcjonariuszy, a w I połowie 2013 r. – 15,6%.

Efektem naszych ustaleń i wniosków było podjęcie decyzji przez ówczesnego Komendanta Głównego Policji o modyfikacji systemu szkolenia i doskonalenia zawodowego w Policji. W rezultacie, w znaczący sposób zwiększono między innymi szkolenia policjantów ruchu drogowego dotyczące udzielania profesjonalnej pierwszej pomocy poszkodowanym w wyniku wypadków drogowych.

W dotychczasowej praktyce prezes NIK niezwykle rzadko i jedynie w najważniejszy sprawach prezentuje Sejmowi wyniki kontroli NIK. Tak było w 2014 r., kiedy przedstawił przygotowaną przez nasz departament „megainformację" dotyczącą bezpieczeństwa ruchu drogowego w Polsce.

Zawarte w nim wnioski i rekomendacje dotyczyły:

• utworzenia na mocy ustawy krajowego Systemu Zarządzania i Kontroli

[25] Megainformacja *Bezpieczeństwo ruchu drogowego*, nr ewid. 148/2014/KPB, listopad 2014 r.

Bezpieczeństwa Ruchu Drogowego oraz powierzenia koordynacji działań w ramach tego systemu jednemu organowi;
• zapewnienia stabilnego finansowania zadań w zakresie bezpieczeństwa ruchu drogowego;
• budowy systemu planowania i analizy efektów podejmowanych działań;
• wprowadzenia niezbędnych zmian w obowiązujących przepisach, w tym między innymi dotyczących automatycznego nadzoru nad ruchem drogowym (tryb nakładania mandatów za przekroczenie prędkości, karanie cudzoziemców dopuszczających się naruszeń przepisów ruchu drogowego);
• modernizacji infrastruktury, ze szczególnym uwzględnieniem rozwiązań w zakresie bezpieczeństwa ruchu drogowego;
• zwiększenia nadzoru nad kwestiami związanymi ze stanem technicznym pojazdów;
• zwiększenia skuteczności działania służb ratowniczych;
• promocji właściwych zachowań wśród uczestników ruchu drogowego.

Niektóre z tych wniosków już zrealizowano. I tak:
• powstało Polskie Obserwatorium Bezpieczeństwa Ruchu Drogowego, gromadzące dane BRD;
• uruchomiono program modernizacji służb mundurowych, w tym Policji (obecnie kontrolowany przez nasz departament);
• zwiększono liczbę policjantów na drogach z ośmiu do dziesięciu tysięcy, jednocześnie intensyfikując szkolenia, o czym wspomniano wyżej;
• zmieniono przepisy dotyczące kontroli stanu technicznego pojazdów;
• trwa rozbudowa automatycznego systemu nadzoru nad ruchem drogowym;
• wyeliminowano wiele nieprawidłowości w funkcjonowaniu poszczególnych skontrolowanych podmiotów.

Trzeba jednak otwarcie przyznać, że w sprawach zasadniczych wiele pozostało jeszcze do zrobienia. Nadal nie możemy powiedzieć, że stworzyliśmy sprawnie działający system bezpieczeństwa ruchu drogowego. Nie wyznaczono wyposażonej w odpowiednie kompetencje instytucji wiodącej. Nie zapewniono stabilnych źródeł finansowania realizacji zadań dotyczących bezpieczeństwa ruchu drogowego. Nie dokończono reorganizacji struktur odpowiedzialnych za funkcjonowanie systemu nadzoru nad ruchem drogowym.

Jednak, podobnie jak we wcześniej opisanych kontrolach, także i tym razem najważniejsze było zwrócenie uwagi na palący problem zapewnienia bezpieczeństwa na polskich drogach. Pomimo zauważalnego postępu, na polskich drogach nadal ginie blisko 3 tysiące ludzi rocznie, co stawia nas na jednym z ostatnich miejsc w Unii Europejskiej.

Zabezpieczenie przeciwpożarowe

Na koniec przybliżę wyniki kontroli naszych poprzedników. Uzmysławiają nam one, jak daleką drogę przebyliśmy Znamienne, że do początku lat dziewięćdziesiątych, gdy dopiero tworzono zręby nowoczesnych instytucji zajmujących się szeroko rozumianym bezpieczeństwem wewnętrznym, NIK w pewnym sensie wchodziła w ich rolę. Moim zdaniem, zarówno sama kontrola, jak i przyjęte do realizacji wnioski dotyczące stanu

zabezpieczenia przeciwpożarowego domów dziecka[26] oraz kontrola stanu zabezpieczenia przeciwpożarowego i ochrony środowiska baz i składów paliwowych[27] zapobiegły nie tylko potencjalnym, ale i realnym zagrożeniom wynikającym wprost z bardzo poważnych nieprawidłowości stwierdzonych przez kontrolerów NIK[28].

Ustalono, że w 17 spośród 20 skontrolowanych domów dziecka określone w przepisach warunki dla dróg ewakuacyjnych nie były spełnione. Odporność ogniowa elementów konstrukcyjnych tych dróg nie zawsze odpowiadała wymaganej klasie. Stosowano palną konstrukcję i wydzielenia dróg ewakuacyjnych. Pod biegami ewakuacyjnych klatek schodowych lokalizowano pomieszczenia gospodarcze, wykonane z materiałów palnych. Stosowano palny wystrój dróg ewakuacyjnych. Ściany korytarzy i klatek schodowych obłożono boazeriami z drewna lub materiałów drewnopochodnych, a podłogi wykładzinami dywanowymi nieposiadającymi atestu niepalności.

W 10 kontrolowanych obiektach utrudniono bądź uniemożliwiono ewakuację w wypadku zagrożenia pożarowego przez zamontowanie nieotwieralnych krat w oknach. Sposób użytkowania klatek schodowych i korytarzy powodował utrudnienie możliwości ewakuacyjnych. Stwierdzono zamykanie na stałe wyjść ewakuacyjnych lub wyłączanie klatek schodowych i części korytarzy z układu komunikacyjnego Ustawiano na nich meble i inne przedmioty, zawężające szerokość dróg ewakuacyjnych. Drzwi wejściowe do budynków otwierały się w kierunku przeciwnym do kierunku ewakuacji. W 10 domach dziecka nie określono zasad organizacji przebiegu ewakuacji oraz zadań dla personelu. Nie przeprowadzano również ćwiczeń.

W II półroczu 1992 r. Najwyższa Izba Kontroli przeprowadziła również kontrolę stanu zabezpieczenia przeciwpożarowego i ochrony środowiska w bazach i składach paliwowych.

Stan techniczny urządzeń dystrybucyjnych w kontrolowanych bazach i składach stwarzał istotne zagrożenie. Instalacje autonalewaków oraz bramownic kolejowych były w znacznym stopniu zużyte technicznie, wskutek czego występowały wycieki produktów naftowych. Z powodu nieszczelności zaworów, do studzienki manipulacyjnej jednego ze zbiorników wyciekał olej napędowy. W składach MON część zbiorników nie była w ogóle wyposażona w armaturę nalewową (krócce) oraz rury odpowietrzające, wskutek czego napełnianie zbiorników następowało bezpośrednio z cystern.

Kontrola wykazała, że jednostki administrujące bazami i składami produktów naftowych nie zawsze przywiązywały wagę do zachowania sprawności i należytego stanu technicznego instalacji uziemiających

[26] ANIK 240/4: *Stan zabezpieczenia przeciwpożarowego Domów Dziecka*.
[27] ANIK 235/8: *Stan zabezpieczenia przeciwpożarowego i ochrony środowiska baz i składów paliwowych*.
[28] Po powołaniu Państwowej Straży Pożarnej, jednym z zadań powierzonych tej formacji był nadzór nad przestrzeganiem przepisów przeciwpożarowych, między innymi w formie czynności kontrolno-rozpoznawczych. Dopiero wówczas podjęto w NIK decyzje o zaprzestaniu realizacji planowych kontroli stanu zabezpieczenia przeciwpożarowego.

i odgromowych, zaniedbując obowiązek przeprowadzania stosownych badań kontrolnych i bieżącego usuwania usterek.

W zlokalizowanych na terenach kompleksów leśnych bazach paliwowych nie zostały wykonane pasy ochronne wokół parków zbiorników oraz urządzenia i instalacje technologiczne uniemożliwiające rozprzestrzenianie się ognia.

W składach wojskowych podziemne zbiorniki posadowione były bezpośrednio w gruncie, bez wykonania pod nimi warstw ochronno-uszczelniających. Samochodowe stanowiska nalewowe zlokalizowano na drogach o nawierzchni żwirowej, nieprzystosowanej do zmywania rozlewisk. Brak utwardzonego podłoża, zabezpieczającego grunt przed przesiąkaniem produktów naftowych, stwierdzono też pod urządzeniami dystrybucyjnymi.

Zaprezentowane wyżej ustalenia, a zwłaszcza realizacja wniosków NIK po kontroli domów dziecka i baz paliwowych potwierdzają wcześniej postawioną tezę, że aktywność Izby w tym obszarze w znaczący sposób przyczyniła się do usunięcia bardzo poważnych nieprawidłowości, których skutki mogłyby okazać się katastrofalne.

Uwagi końcowe

W opracowaniu starałem się przybliżyć wyniki kontroli, które – choć w różnym stopniu – wywarły realny wpływ na poprawę stanu bezpieczeństwa wewnętrznego w naszym kraju.

Ze względu na ograniczone ramy artykułu, z konieczności pominąłem wiele równie ważnych badań przeprowadzonych przez Departament Porządku i Bezpieczeństwa Wewnętrznego, których wyniki przyczyniły się do konkretnych zmian w prawie i usprawniły działania służb odpowiedzialnych za ten ważny dla państwa obszar. Jest to powód do satysfakcji zarówno obecnych kontrolerów, jak i naszych poprzedników.

MAREK BIEŃKOWSKI
p.o. dyrektor Departamentu Porządku i Bezpieczeństwa Wewnętrznego NIK

Słowa kluczowe: stulecie NIK, jubileusz, bezpieczeństwo wewnętrzne kraju, Policja, służby specjalne, cyberbezpieczeństwo, ochrona przeciwpożarowa

Key words: centenary of NIK, jubilee, internal security of the country, Police, special services, cyber security, fire protection