



NAJWYŻSZA IZBA KONTROLI

KPB.430.1.2025

Nr ewid. 13/2025/P/24/033/KPB

Informacja o wynikach kontroli

FUNKCJONOWANIE SYSTEMU ŁĄCZNOŚCI W SŁUŻBACH PODLEGŁYCH MSWIA

MISJA

Najwyższej Izby Kontroli jest niezależna, profesjonalna kontrola zadań publicznych w interesie obywateli i państwa

Dyrektor Departamentu Porządku
i Bezpieczeństwa Wewnętrznego

Tomasz Sordyl

/podpisano elektronicznie/

Wiceprezes Najwyższej Izby Kontroli

Michał Jędrzejczyk

/podpisano elektronicznie/

Prezes Najwyższej Izby Kontroli

Marian Banaś

/podpisano elektronicznie/

Warszawa, maj 2025 r.

Najwyższa Izba Kontroli

ul. Filtrowa 57

02-056 Warszawa

+48 22 444 50 00

nik@nik.gov.pl

www.nik.gov.pl

Spis treści

Wykaz skrótów, skrótowców i pojęć	5
1. Wprowadzenie	8
2. Ocena ogólna	10
3. Synteza	12
4. Wnioski	19
5. Ważniejsze wyniki kontroli	21
5.1. Brak jednolitego systemu łączności radiowej dla służb porządku i bezpieczeństwa wewnętrznego	21
5.1.1. Dotychczasowe działania na rzecz wdrożenia jednolitego systemu łączności radiowej dla służb MSWiA.....	21
5.1.2. Niepowodzenie przedsięwzięcia budowy Ogólnokrajowego Cyfrowego Systemu Łączności Radiowej	24
5.1.3. Perspektywy wdrożenia jednolitego systemu łączności w świetle ustawy o ochronie ludności i obronie cywilnej.....	26
5.2. Funkcjonowanie systemów łączności radiowej w poszczególnych służbach	29
5.2.1. Policja.....	30
5.2.2. Państwowa Straż Pożarna.....	33
5.2.3. Straż Graniczna.....	36
5.2.4. Służba Ochrony Państwa.....	39
5.2.5. Szkolenie i wyposażenie funkcjonariuszy	39
5.2.6. Dług technologiczny w systemach łączności służb podległych MSWiA.....	42
5.2.7. Wykorzystywanie telefonii komórkowej przez służby	48
5.2.8. Problemy kadrowe w zakresie obsługi systemów teleinformatycznych.....	50
5.2.9. Niedostateczne przygotowanie systemów łączności na sytuacje kryzysowe	53
5.2.10. Przeglądy techniczne masztów i instalacji antenowych	56
5.3. Interoperacyjność systemów łączności radiowej.....	58
5.3.1. Kanał B112	58
5.3.2. Wykorzystanie systemu TETRA przez służby	60
5.3.3. Współpraca służb w warunkach braku jednolitego systemu łączności	61

5.4. Nadzór Ministra SWiA.....	64
6. Załączniki.....	67
6.1. Metodyka kontroli i informacje dodatkowe.....	67
6.1.1. Wykaz ocen kontrolowanych jednostek.....	72
6.2. Analiza stanu prawnego i uwarunkowań organizacyjno-ekonomicznych	75
6.3. Wykaz aktów prawnych dotyczących kontrolowanej działalności	77
6.4. Wykaz podmiotów, którym przekazano informację o wynikach kontroli.....	79

WYKAZ SKRÓTÓW, SKRÓTOWCÓW I POJĘĆ

- CTCSS** Continuous Tone Coded-Squelch System – system zabezpieczeń dźwiękowych stosowany w radiokomunikacji, mający na celu eliminację niechcianych sygnałów i szumów, co umożliwia komunikację jedynie między urządzeniami ustawionymi na ten sam ton.
- CSR** Cyfrowy System Radiokomunikacyjny.
- DMR** Digital Mobile Radio – standard cyfrowej radiokomunikacji mobilnej opracowany przez ETSI. Został zaprojektowany w celu zapewnienia prostych, ekonomicznych i wydajnych systemów radiowych dla użytkowników profesjonalnych. Oferuje różne tryby pracy: TIER I, TIER II i TIER III, co pozwala na elastyczne dopasowanie rozwiązań radiokomunikacyjnych do potrzeb użytkowników. Standard ten może funkcjonować z istniejącymi systemami analogowymi, co umożliwia płynne przejście z technologii analogowej na cyfrową.
- EDACS** Enhanced Digital Access Communication System – oferowany przez firmę Ericsson system trunkingowy, umożliwiający cyfrową transmisję danych oraz cyfrową lub analogową transmisję sygnałów mowy w kanale radiowym. Bez dodatkowych komponentów nie umożliwia jednak szyfrowania komunikacji.
- ETSI** European Telecommunications Standards Institute – niezależna, niekomercyjna organizacja standaryzacyjna, założona w 1988 r. z inicjatywy Komisji Europejskiej. Zajmuje się rozwijaniem globalnych standardów technicznych dla systemów, aplikacji i usług telekomunikacyjnych, wspierając tym samym europejskie regulacje i ustawodawstwo.
- KG PSP** Komenda Główna Państwowej Straży Pożarnej.
- KGSG** Komenda Główna Straży Granicznej.
- KGP** Komenda Główna Policji.
- KP/KM** Komenda Powiatowa/Komenda Miejska.
- MSWiA** Ministerstwo Spraw Wewnętrznych i Administracji.
- Minister SWiA** Minister Spraw Wewnętrznych i Administracji.
- NEXEDGE** Cyfrowy system łączności radiowej opracowany przez firmę Kenwood, bazujący na protokole NXDN. Dedykowany jest m.in. służbom bezpieczeństwa publicznego. Od 2012 r. NXDN jest standardem otwartym. Umożliwia pracę w trybie konwencjonalnym.
- OCSŁR** Ogólnokrajowy Cyfrowy System Łączności Radiowej.

OSG	Oddział Straży Granicznej.
Program modernizacji Policji 2022–2025	Ustawa z dnia 17 grudnia 2021 r. o ustanowieniu „Programu modernizacji Policji, Straży Granicznej, Państwowej Straży Pożarnej i Służby Ochrony Państwa w latach 2022–2025”, o ustanowieniu „Programu modernizacji Służby Więziennej w latach 2022–2025” oraz o zmianie ustawy o Policji i niektórych innych ustaw (Dz.U. z 2024 r., poz. 86).
SOP	Służba Ochrony Państwa.
SRP-T	System Radiowy Policji – TETRA.
TETRA	Terrestrial Trunked Radio – standard cyfrowej radiokomunikacji opracowany przez ETSI, przeznaczony dla służb ratunkowych, wojska oraz innych organizacji wymagających niezawodnej i zabezpieczonej komunikacji. Standard oferuje szeroki zakres funkcji, w tym grupową komunikację głosową, transmisję danych, wiadomości tekstowe oraz pełne wsparcie dla usług trunkingowych, co pozwala na efektywne zarządzanie zasobami sieci radiowej. TETRA jest znana z wysokiego poziomu bezpieczeństwa.
TIER I, TIER II i TIER III	Klasyfikacja TIER opiera się na poziomach dostępności usług. Im wyższy poziom, tym większa dostępność i odporność na awarie i incydenty, ale również wyższe koszty systemu.
Tranking	Metoda używania niewielkiej liczby kanałów telekomunikacyjnych przez dużą liczbę potencjalnych użytkowników. Dzięki organizacji systemu opartej na strukturze logicznych grup rozmównych możliwe jest współużytkowanie systemu trunkingowego przez wiele niezależnych grup użytkowników.
Ustawa o finansach publicznych lub ufp	Ustawa z dnia 27 sierpnia 2009 r. o finansach publicznych (Dz. U. z 2024 r. poz. 1530, ze zm.).
Ustawa o nadzorze	Ustawa z dnia 21 czerwca 1996 r. o szczególnych formach sprawowania nadzoru przez ministra właściwego do spraw wewnętrznych (Dz. U. 2024 r., poz. 309, ze zm.).
Ustawa o NIK	Ustawa z dnia 23 grudnia 1994 r. o Najwyższej Izbie Kontroli (Dz. U. z 2022 r. poz. 623).
Ustawa o Policji	Ustawa z dnia 6 kwietnia 1990 r. o Policji (Dz. U. z 2024 r. poz. 145, ze zm.).
VHF	Very High Frequency – zakres częstotliwości radiowych obejmujący przedział od 30 MHz do 300 MHz. Zakres VHF jest często wykorzystywany w komunikacji radiowej, transmisji telewizyjnej oraz w różnych systemach bezprzewodowych, takich jak systemy nawigacyjne i radarowe. Długość fali w zakresie VHF umożliwia

stosunkowo dobre przenikanie przez przeszkody, a także pozwala na osiągnięcie zadowalających odległości transmisji przy stosunkowo niskich poziomach mocy.

Zarządzenie nr 22 Zarządzenie nr 22 Komendanta Głównego Policji z dnia 14 lipca 2020 r. w sprawie określenia metod i form wykonywania zadań Policji z użyciem środków łączności radiowej (Dz. Urz. KGP poz. 38).
KGP

Zarządzenie nr 33 Zarządzenie nr 33 Komendanta Głównego Straży Granicznej z dnia 2 sierpnia 2011 r. w sprawie łączności radiowej w systemach ultrakrótkofalowej łączności radiowej przy wykonywaniu zadań w jednostkach organizacyjnych Straży Granicznej (Dz. Urz. KGSG Nr 9, poz. 36).
KGSG

1. WPROWADZENIE

Pytanie definiujące cel główny kontroli

Czy system łączności w kontrolowanych jednostkach funkcjonuje właściwie?

Pytania definiujące cele szczegółowe kontroli

1. Czy przyjęte koncepcje i zasady funkcjonowania łączności radiowej w służbach podległych Ministrowi Spraw Wewnętrznych i Administracji odpowiadały ustalonym standardom w obszarze bezpieczeństwa, porządku publicznego i ratownictwa oraz były ze sobą spójne?

2. Czy wykorzystywane przez służby podległe Ministrowi SWiA systemy łączności pozwalały im na skuteczną komunikację odpowiadającą wymogom i zagrożeniom współczesności?

3. Czy wykorzystywane przez służby podległe Ministrowi SWiA systemy łączności były ze sobą kompatybilne i umożliwiały bezpieczną i skuteczną współpracę pomiędzy formacjami w sytuacji kryzysowej?

Jednostki

kontrolowane

MSWiA, KGP, KG SG, KG PSP, SOP, a także KW Policji, KW PSP, oddziały SG (łącznie 15) oraz KM/KP Policji i PSP (łącznie 10)

Jednostki objęte

badaniem

kwestionariuszowym

Funkcjonariusze służb podległych MSWiA

Okres objęty kontrolą

Od 1 stycznia 2022 r. do 31 października 2024 r.¹

Służby podległe Ministrowi Spraw Wewnętrznych i Administracji – Policja, Państwowa Straż Pożarna, Straż Graniczna oraz Służba Ochrony Państwa – odgrywają kluczową rolę w systemie bezpieczeństwa wewnętrznego. Ich zadania obejmują ochronę życia i mienia obywateli, zabezpieczenie granic, reagowanie na zagrożenia pożarowe oraz ochronę najważniejszych osób i obiektów państwowych. Skuteczna realizacja tych obowiązków wymaga sprawnego systemu łączności radiowej, który zapewnia szybki i niezawodny przepływ informacji, a tym samym umożliwia efektywną koordynację działań, zwłaszcza w sytuacjach kryzysowych.

Zgodnie z zasadą, że przepływ informacji odgrywa kluczową rolę w skutecznej realizacji działań – system łączności stanowi podstawowy element umożliwiający realizację ww. zadań. System ten integruje różne elementy operacyjne, zapewniając ich spójne i efektywne funkcjonowanie. Łączność umożliwia koordynację i synchronizację działań, przekazywanie informacji i rozkazów, monitorowanie zasobów i reagowanie na zmieniającą się sytuację. Bez sprawnej łączności radiowej nie można dziś sobie wyobrazić skutecznej pracy formacji odpowiedzialnych za bezpieczeństwo wewnętrzne.

Najwyższa Izba Kontroli od kilku lat analizowała niepokojące informacje, mogące świadczyć o tym, że system łączności w służbach nie działa wystarczająco skutecznie. W styczniu 2017 r. na autostradzie A1 koło Piotrkowa Trybunalskiego, podczas skrajnie trudnych warunków pogodowych, doszło do karambolu, w którym zderzyło się 76 samochodów. Po pierwszym karambolu nastąpił w pobliżu kolejny o mniejszych skutkach, ale także wymagający interwencji służb. Autostrada była zablokowana przez 15 godzin z obu stron. W ratowaniu poszkodowanych udział wzięło łącznie 100 policjantów, 70 strażaków, dwa helikoptery i wiele karetek. Podczas konferencji prasowej po zakończeniu akcji ratunkowej pierwszym przekazanym wnioskiem była informacja o problemach w łączności pomiędzy służbami. Ich powodem był brak zintegrowanego systemu łączności – służby dysponowały niezależnymi systemami opartymi na niekompatybilnych standardach. Ponadto w poszczególnych obszarach kraju te same służby miały przydzielone różne częstotliwości. Sytuacja ta uniemożliwiała szybkie uruchomienie połączeń do współpracy w postaci bezpośredniej komunikacji. Z kolei w 2019 r. dziennikarze ujawnili, że można podsłuchiwać służby zabezpieczające trasy przejazdu najważniejszych osób w państwie za pomocą sprzętu wartego kilkaset złotych. Powodem był fakt, że używały

¹ Z wykorzystaniem dowodów wytworzonych przed i po tym okresie, związanych z przedmiotem tej kontroli.

one przestarzałych i nieodpowiednio zabezpieczonych systemów łączności radiowej, które nie zmieniły się od wielu lat.

Próby stworzenia kompletnego, nowoczesnego systemu łączności służb ratowniczych i porządku publicznego w Polsce rozpoczęły się przeszło 20 lat temu, jednakże dotychczas nie przyniosły oczekiwanych rezultatów. Pomimo trwającej, prowadzonej przez poszczególne służby modernizacji, istniejące systemy nadal nie spełniają niezbędnych wymagań w zakresie mobilności, trwałości, niezawodności i bezpieczeństwa przekazywanych informacji, a także koordynacji sił i środków w sytuacjach szczególnych zarówno w skali lokalnej, jak i krajowej.

Na problem ten, niejako przy okazji systemowej analizy badanych obszarów, kilkakrotnie wskazywała NIK w prowadzonych kontrolach problemowych (m.in. P/17/019 *Ochrona ludności w ramach zarządzania kryzysowego i obrony cywilnej*² oraz P/22/029 *Przygotowanie państwa na zagrożenia związane z działaniami hybrydowymi*³). Sformułowane wówczas wnioski pokontrolne nie zostały jednak zrealizowane.

Mając na uwadze opisane powyżej okoliczności, NIK zdecydowała o przeprowadzeniu kompleksowej kontroli, ukierunkowanej wprost na problematykę funkcjonowania systemów łączności. Jej celem było zweryfikowanie, czy wykorzystywane przez służby systemy łączności radiowej działają właściwie i umożliwiają im sprawne i skuteczne realizowanie powierzonych zadań. Założeniem kontroli było również sprawdzenie, czy systemy te odpowiadają wymaganiom współczesności, zarówno pod względem funkcjonalności, jak i bezpieczeństwa informacji. Izba przyjrzała się także temu, czy systemy łączności radiowej umożliwiają służbom współdziałanie, co jest szczególnie istotne w sytuacjach kryzysowych oraz może okazać się bezwzględnie konieczne w przypadku wystąpienia zdarzeń skutkujących koniecznością uruchomienia obrony cywilnej.

² Zob.: <https://www.nik.gov.pl/kontrole/P/17/039/>

³ Zob.: <https://www.nik.gov.pl/kontrole/P/22/029/>

2. OCENA OGÓLNA

**Brak wspólnego
cyfrowego systemu
łączności utrudniał
efektywne
współdziałanie służb,
szczególnie
w sytuacjach
wymagających
natychmiastowej
reakcji
i skoordynowanych
działań**

System łączności radiowej w służbach podległych Ministrowi SWiA nie funkcjonuje właściwie. Przeprowadzona kontrola wykazała liczne nieprawidłowości w tym obszarze, które mogą negatywnie wpływać na skuteczność operacyjną służb oraz ich zdolność do szybkiego i adekwatnego reagowania na sytuacje nadzwyczajne. Efektywna komunikacja jest bowiem kluczowym elementem sprawnego reagowania na zagrożenia, a jej niewydolność stanowi istotne ryzyko dla bezpieczeństwa publicznego.

Najistotniejszym problemem w tym obszarze funkcjonowania państwa jest brak jednolitego, cyfrowego systemu łączności. Pomimo prowadzonych od co najmniej 20 lat prac analitycznych i koncepcyjnych, ze względu na niezapewnienie stabilnego finansowania oraz brak koordynacji działań ze strony MSWiA, wdrożenie tego systemu wciąż pozostaje niezrealizowanym celem. Dotychczasowe prowizoryczne rozwiązania, takie jak analogowa sieć współdziałania (kanał B112), były wykorzystywane przez służby jedynie sporadycznie z uwagi na niski poziom techniczny i brak odpowiednich zabezpieczeń.

W sytuacji niewdrożenia jednolitego, cyfrowego systemu łączności radiowej każda ze służb opracowała własną koncepcję – zgodną wprawdzie z uznanymi standardami – jednak realizowaną niezależnie od pozostałych służb MSWiA, co doprowadziło do braku kompatybilności między systemami. W konsekwencji komunikacja między służbami jest utrudniona, szczególnie w sytuacjach wymagających szybkiej wymiany informacji i skoordynowanych działań. Jedynie Straż Graniczna i Służba Ochrony Państwa w pełni wdrożyły cyfrowe systemy łączności, Państwowa Straż Pożarna dopiero rozpoczyna proces budowy takiego systemu, a Policja jest w trakcie jego realizacji, choć jako jedyna ze służb MSWiA robi to w docelowym standardzie TETRA. NIK zwraca uwagę, że służby podległe MSWiA nie wymieniały się informacjami o działaniach w zakresie budowy lub rozbudowy systemów łączności radiowej, co skutkowało brakiem kompatybilności oraz uniemożliwiało wykorzystanie efektu skali i współdzielenie infrastruktury. Prowadziło to do zwiększenia kosztów, ponieważ realizowano szereg odrębnych, mniejszych zamówień i zamiast np. korzystać z istniejących masztów czy radiolinii, służby budowały własne, niezależne obiekty. W efekcie w okresie objętym kontrolą większość funkcjonariuszy wciąż wykorzystywała przestarzałą technologię analogową, co utrudniało skuteczną komunikację i ograniczało niezawodność oraz bezpieczeństwo systemu łączności.

Dopiero utworzenie Systemu Bezpiecznej Łączności Państwowej, z podsystemem radiowej łączności w standardzie TETRA, którego ramy prawne i organizacyjne zawarto w uchwalonej w 2024 r. z inicjatywy MSWiA ustawie o ochronie ludności i obronie cywilnej, doprowadzić ma do rzeczywistej integracji systemów komunikacji w służbach oraz zachowania ich skuteczności operacyjnej w sytuacjach kryzysowych. NIK zauważa jednak, że wdrożenie takie ma być możliwe w perspektywie co najmniej sześciu lat, zakładając, że nie dojdzie do nieprzewidzianych opóźnień. W ocenie NIK istotnym zagrożeniem dla realizowanego projektu może być, oprócz samej skali i skomplikowania realizowanego przedsięwzięcia, m.in. brak niezbędnej liczby administratorów oraz specjalistów odpowiedzialnych za obsługę systemów radiowej łączności cyfrowej. W związku z powyższym, biorąc pod uwagę dotychczasowe doświadczenia w zakresie realizacji tego rodzaju projektów oraz narastające wyzwania w zakresie bezpieczeństwa wewnętrznego, w ocenie NIK konieczne jest dołożenie najwyższej staranności, aby jak najszybciej wdrożyć nowoczesny system łączności cyfrowej dla służb podległych MSWiA oraz jednostek obrony cywilnej i ochrony ludności.

3. SYNTEZA

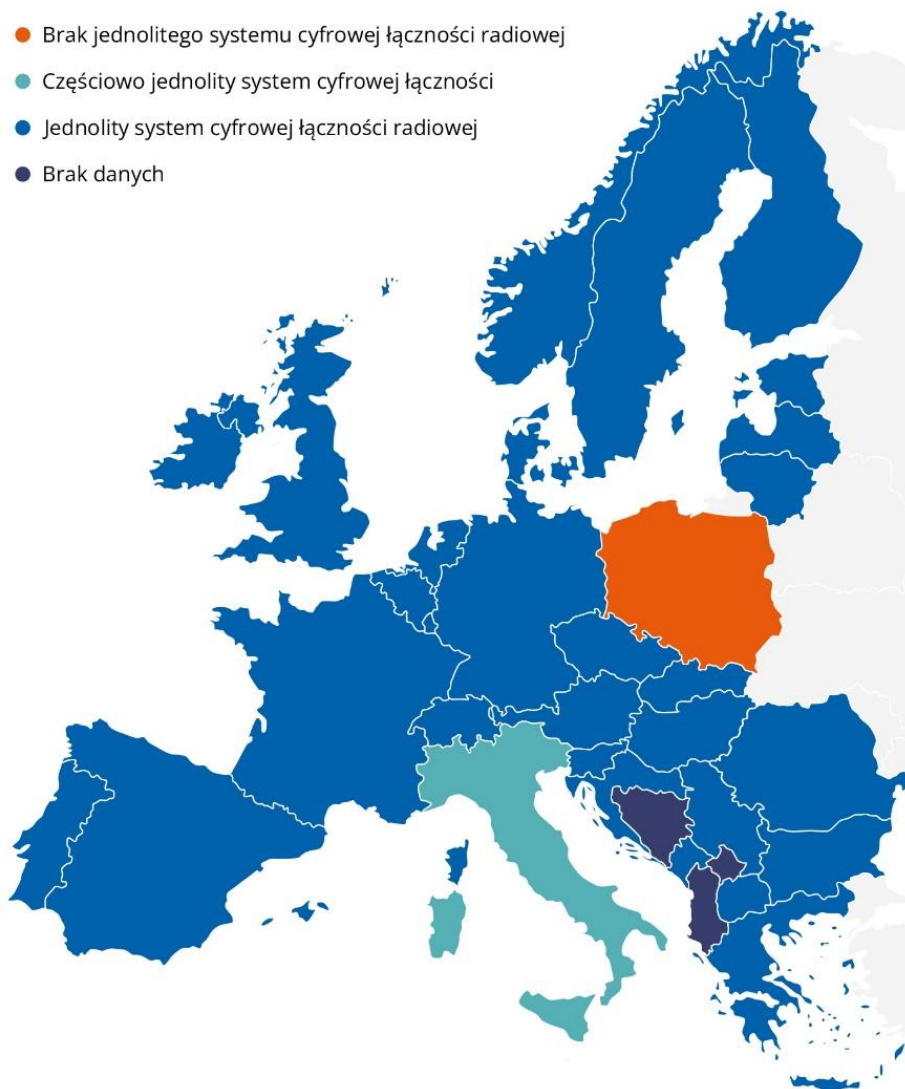
Brak jednolitego systemu cyfrowej łączności radiowej

Ministrowi Spraw Wewnętrznych i Administracji, pomimo podejmowanych od wielu lat prób i trwających prac analityczno-koncepcyjnych, nie udało się doprowadzić do wdrożenia ogólnokrajowego cyfrowego systemu łączności radiowej dla podległych mu służb działających w obszarze bezpieczeństwa wewnętrznego i ratownictwa. System ten ma kluczowe znaczenie dla zapewnienia efektywnego współdziałania funkcjonariuszy, zwłaszcza w sytuacjach kryzysowych, a jego istnienie jest przyjętym standardem w państwach europejskich. [str. 21–24; 60–65]

Infografika nr 1

Ogólnokrajowe cyfrowe systemy radiowe w Europie

- Brak jednolitego systemu cyfrowej łączności radiowej
- Częściowo jednolity system cyfrowej łączności
- Jednolity system cyfrowej łączności radiowej
- Brak danych



Źródło: opracowanie własne NIK na podstawie danych przekazanych przez MSWiA.

**Brak dedykowanego
mechanizmu
finansowania**

Próby wdrożenia jednolitego cyfrowego systemu łączności radiowej dla służb podległych MSWiA w oparciu o zasoby i system łączności Policji⁴ nie powiodły się, przede wszystkim z powodu braku dedykowanego wieloletniego mechanizmu finansowania przeznaczonego dla takiego zadania. Zabrakło również koordynatora, który byłby umocowany na poziomie wyższym niż Komendant Główny Policji, mogącego realnie kierować budową systemu przeznaczonego dla ogółu służb i instytucji państwowych na terenie całego kraju. [str. 24–25]

**Służby rozwijały
systemy łączności
niezależnie od siebie**

W tej sytuacji służby rozwijały i utrzymywały własne, odrębne systemy łączności radiowej, pracujące w odmiennych standardach, często ze sobą niekompatybilnych. Straż Graniczna wdrożyła – jako podstawowy – system łączności w oparciu o standard DMR, SOP – w oparciu o standard NEXEDGE, Państwowa Straż Pożarna opracowała w 2022 r. koncepcję migracji do systemu cyfrowej łączności w oparciu o standard DMR, ale wciąż używała łączności analogowej, a Policja wprowadziła jako podstawowy system SRP-TETRA, ale w przeważającej części wciąż opierała się na łączności analogowej oraz standardzie DMR (który ze względu na swoje ograniczenia oraz indywidulane, niezależne implementacje nie zapewnił interoperacyjności). Stwarzało to realne ryzyko braku efektywnego współdziałania służb podległych MSWiA w czasie reagowania na występujące zagrożenia. Ponadto służby podległe MSWiA nie wymieniały się informacjami o działaniach w zakresie budowy lub rozbudowy systemów łączności radiowej, co skutkowało brakiem kompatybilności oraz uniemożliwiało wykorzystanie efektu skali i współdzielenie infrastruktury. Prowadziło to do zwiększenia kosztów, ponieważ realizowano szereg odrębnych, mniejszych zamówień i zamiast np. korzystać z istniejących masztów czy radiolinii, służby budowały własne, niezależne obiekty. [str. 29–38]

**Służby używały sieci
analogowych, które
nie spełniały wymagań
bezpieczeństwa**

W Państwowej Straży Pożarnej, Policji, a częściowo także w Służbie Ochrony Państwa wciąż istniała konieczność korzystania z urządzeń i sieci analogowych, które nie spełniają wymagań stawianych systemom łączności radiowej przeznaczonych dla służb porządku publicznego i ratownictwa w zakresie bezpieczeństwa, interoperacyjności i zasięgu. Większość dedykowanych radiotelefonów pracujących w tych sieciach była wyeksploatowana i przestarzała technologicznie. O zmniejszającej się funkcjonalności technologii analogowej świadczy fakt, iż służby nie miały możliwości zakupu nowych radiotelefonów analogowych, ponieważ nie były one już dostępne na rynku. W rezultacie zmuszone były nabywać radiotelefony cyfrowe w standardzie DMR, które musiały być

⁴ Minister SWiA powierzył Komendantowi Głównemu Policji w 2017 r. zadanie budowy jednolitego systemu cyfrowej łączności radiowej struktur zarządzania kryzysowego i służb ratowniczych.

**Kanał współpracy
służb (B112) nie
zapewnił możliwości
skutecznego
współdziałania**

skonfigurowane do obsługi sieci analogowej w celu zapewnienia kompatybilności z istniejącą infrastrukturą. [str. 42–47]

Udostępniona przez MSWiA analogowa sieć współdziałania (kanał B112) wykorzystywana była we wspólnych działaniach służb incydentalnie, głównie z powodu niskiego poziomu technicznego i braku odpowiednich zabezpieczeń. Brak możliwości szyfrowania transmisji sprawiał, że komunikacja na kanale B112 była podatna na podsłuch i zakłócenia. Niski poziom zaufania do jego niezawodności sprawiał, że służby unikały korzystania z niego, wybierając inne rozwiązania. Najczęściej wymieniano się oficerami łącznikowymi oddelegowanymi do sztabów, przekazywano radiotelefony jednej ze służb funkcjonariuszom innych formacji MSWiA lub też używano służbowych bądź prywatnych telefonów komórkowych. W każdej ze służb panowało przekonanie, że aby zwiększyć efektywność współdziałania, konieczne jest zastąpienie kanału B112 nowoczesnym, cyfrowym systemem łączności, który spełniałby współczesne wymagania w zakresie bezpieczeństwa, niezawodności i kompatybilności. [str. 59–60]

**Służby wspierają się
cywilną telefonią
komórkową**

Telefonia komórkowa, pomimo że nie została zaprojektowana jako podstawowy środek komunikacji operacyjnej, w praktyce pełniła rolę uzupełniającą wobec dedykowanych systemów łączności radiowej. Stopień wykorzystania telefonii komórkowej wzrastał proporcjonalnie do ograniczeń i niedostatków funkcjonalnych systemu radiowego, który w wielu przypadkach nie spełniał wymagań w zakresie niezawodności, bezpieczeństwa oraz efektywności współpracy między służbami. Komunikacja komórkowa realizowana była co do zasady za pomocą telefonów służbowych, choć dopuszczano również wykorzystanie telefonów prywatnych, szczególnie jeśli niedostępny był dedykowany system łączności, a funkcjonariusz nie był wyposażony w telefon służbowy. Takie wykorzystanie telefonów komórkowych może prowadzić – szczególnie w sytuacji kryzysowej lub konieczności uruchomienia obrony cywilnej – do opóźnień, zakłóceń w komunikacji, zagrożenia samych funkcjonariuszy i poważnych konsekwencji dla bezpieczeństwa publicznego. [str. 48–50]

**Brak przepisów
dotyczących
zachowania zasięgu
w budynkach**

Kontrola wykazała trudności w zapewnieniu skutecznej łączności w obiektach, których architektura, ze względu na efekt tzw. klatki Faradaya⁵, uniemożliwia skuteczną propagację fal radiowych. Problemy te nie występują w budynkach, gdzie wdrożono systemy retransmisji sygnału radiowego na potrzeby służb. NIK zwraca uwagę na brak regulacji prawnych

⁵ Konstrukcja taka ze względu na wykonanie z przewodzącego materiału (np. siatki metalowej lub blachy) skutecznie blokuje fale elektromagnetyczne, co uniemożliwia odbiór i nadawanie sygnałów radiowych wewnątrz niej. W konsekwencji w budynkach o takiej konstrukcji sygnał radiowy, telefoniczny i Wi-Fi może być osłabiony lub całkowicie zablokowany.

**Systemy łączności są
niedostatecznie
przygotowane do
sytuacji kryzysowych**

dotyczących stosowania urządzeń i rozwiązań technicznych, które umożliwiałyby odpowiednią propagację sygnału radiowego w miejscach, gdzie z uwagi na charakter konstrukcji mogą występować zakłócenia w zasięgu systemów łączności wykorzystywanych przez służby. [str. 33–34]

Wyniki kontroli wskazały na ogólny problem niedostatecznego przygotowania systemów łączności radiowej, wykorzystywanych przez służby podległe MSWiA, do funkcjonowania w sytuacjach kryzysowych. Obecne rozwiązania techniczne i organizacyjne nie zapewniają w pełni niezawodnej komunikacji w warunkach zakłóceń infrastrukturalnych, takich jak awarie, klęski żywiołowe czy zagrożenia wynikające z działań wojennych. Powódź na Dolnym Śląsku w 2024 roku ujawniła poważne braki w systemie łączności, gdy wskutek zalania i braku zasilania wyłączyły się stacje bazowe w Kotlinie Kłodzkiej. Przerwy w działaniu sieci telefonii komórkowej utrudniły koordynację służb ratunkowych oraz organizację pomocy dla poszkodowanych. PSP musiała improwizować, łącząc radioprzemienniki DMR i korzystając z terminali satelitarnych Starlink, które trzeba było pozyskiwać od innych podmiotów ze względu na ich niewystarczającą liczbę. [str. 53–56]

**Zaniedbywane
przeglądy instalacji
antenowych**

Zidentyfikowano szereg nieprawidłowości związanych z wymaganymi okresowymi przeglądami technicznymi masztów i instalacji antenowych wykorzystywanych przez dwie najliczniejsze służby – Policję i Państwową Straż Pożarną. Kontrola jednostek właściwych do wykonywania takich przeglądów wykazała zaniechania w czterech spośród pięciu skontrolowanych jednostek Policji oraz czterech spośród pięciu skontrolowanych jednostek PSP.

Obowiązek ww. przeglądów wynika z art. 62 ust. 1 pkt 1 ustawy Prawo budowlane, który nakłada na właściciela lub zarządcę obiektu budowlanego obowiązek corocznego sprawdzenia stanu technicznego elementów budowli narażonych na szkodliwe wpływy atmosferyczne i inne czynniki mogące powodować ich degradację. Zaniedbywanie tego obowiązku – ze względu na wagę i rozmiary przynajmniej części takich instalacji antenowych – może prowadzić do obniżenia poziomu bezpieczeństwa użytkowania obiektu oraz zagrożenia dla zdrowia i życia ludzkiego. [str. 57–58]

**Zintegrowany system
łączności wzmacnia
potencjał służb**

Kontrola wykazała, że służby potrafiły skutecznie wykorzystać możliwości nowoczesnego systemu trunkingowego TETRA, dedykowanego zapewnieniu bezpiecznej i efektywnej łączności radiowej. System taki uruchomiono dotychczas w czterech miastach: Łodzi, Krakowie, Szczecinie oraz Warszawie. Dzięki włączeniu do niego podmiotów podległych Urzędowi Miasta, Wojewodzie Mazowieckiemu oraz Państwowej Straży Pożarnej osiągnięto w stolicy interoperacyjność pomiędzy służbami. Utworzenie sieci RATUNEK, opartej na policyjnym systemie TETRA,

umożliwiło bieżącą współpracę m.in. Policji, Straży Pożarnej, Pogotowia Ratunkowego, Straży Miejskiej oraz centrów zarządzania kryzysowego. Rozwiązanie to jest przykładem docelowego wykorzystania jednolitego systemu cyfrowej łączności radiowej i stanowi modelową, dobrą praktykę, która ilustruje, jak mogłyby działać służby po wprowadzeniu jednolitego systemu łączności radiowej na terenie całego kraju. [str. 60–61]

**Trudności
w pozyskaniu
administratorów
systemów łączności**

W trakcie kontroli stwierdzono, że w każdej z badanych służb występuje problem związany z niedostateczną liczbą administratorów lub specjalistów odpowiedzialnych za obsługę systemów radiowej łączności cyfrowej. Ponadto zidentyfikowano trudności w pozyskiwaniu wykwalifikowanego personelu, co stanowi istotne wyzwanie w kontekście planowanego rozwoju tych systemów. Braki kadrowe mogą negatywnie wpłynąć na bieżące utrzymanie, niezawodność oraz efektywność realizacji projektów modernizacyjnych, a także na podjęcie przedsięwzięć związanych z budową Systemu Bezpiecznej Łączności Państwowej. Ustalono, że służby korzystały z dodatku teleinformatycznego, jednak według oceny NIK zasady jego przyznawania nie były dostatecznie ujednolicone i wystandardyzowane. Brak spójnych kryteriów mógł prowadzić do nierównego traktowania pracowników zatrudnionych w różnych formacjach. Ponadto stwierdzono, że Państwowa Straż Pożarna (PSP) nie miała możliwości skorzystania z tego dodatku, co dodatkowo pogłębiało trudności w pozyskiwaniu oraz utrzymywaniu wykwalifikowanych specjalistów w tej służbie.

Współczesne systemy radiowej łączności cyfrowej są coraz bardziej zintegrowane z obszarem IT, co zwiększa ich podatność na potencjalne cyberataki. Brak odpowiednich specjalistów, odpowiedzialnych za zarządzanie ryzykiem cybernetycznym, może stanowić istotne zagrożenie dla ciągłości i bezpieczeństwa komunikacji służb. [str. 50–53]

**Szkolenie
i wyposażenie
funkcjonariuszy**

Funkcjonariuszom każdej z kontrolowanych służb zapewniono szkolenia oraz wyposażenie niezbędne do obsługi systemów łączności radiowej. Jednocześnie stwierdzono niedostateczne wyposażenie niektórych jednostek Policji, szczególnie w sprzęt do łączności cyfrowej. Choć zidentyfikowane zasoby były wystarczające do realizacji codziennych zadań w ramach służby zmianowej, mogły okazać się niewystarczające w sytuacji kryzysowej, wymagającej pełnej mobilizacji wszystkich funkcjonariuszy. [str. 39–42]

**Niewystarczający
nadzór Ministra Spraw
Wewnętrznych
i Administracji**

W ocenie NIK nadzór Ministra Spraw Wewnętrznych i Administracji nad realizacją zadań związanych z organizacją i funkcjonowaniem systemów łączności radiowej w podległych służbach nie był w całym okresie objętym kontrolą prowadzony w sposób rzetelny. Minister nie dysponował pełnymi informacjami dotyczącymi problemów związanych z użytkowanymi systemami łączności oraz trudnościami, jakie występowały w czasie

działań podejmowanych w sytuacjach kryzysowych. Nie miał też wiedzy o przyjętej w PSP koncepcji migracji do łączności cyfrowej DMR. Zadania z zakresu planowania i organizacji łączności radiowej powierzono Departamentowi Teleinformatyki, który jednak nie dysponował wystarczającymi zasobami kadrowymi, w szczególności specjalistami z zakresu radiokomunikacji, co uniemożliwiało skuteczne wykonywanie powierzonych obowiązków. Dodatkowo formalny nadzór nad służbami resortu, sprawowany przez inne komórki organizacyjne MSWiA zgodnie z regulaminem organizacyjnym, nie obejmował kwestii związanych z organizacją łączności radiowej, co stanowiło istotną lukę w strukturze nadzoru. [str. 65–67]

**Ustawa o ochronie
ludności szansą na
wdrożenie
skutecznego systemu
łączności radiowej**

Minister, realizując m.in. wniosek Najwyższej Izby Kontroli, podjął w 2024 r. działania na rzecz utworzenia Systemu Bezpiecznej Łączności Państwowej (SBŁP), z podsystemem radiowej łączności trunkingowej w standardzie TETRA. Podsystem ten ma spełnić rolę jednolitego systemu cyfrowej łączności radiowej struktur zarządzania kryzysowego i służb ratowniczych. Ramy prawne i organizacyjne zawarto dla niego w ustawie o ochronie ludności i obronie cywilnej. Zapewnia ona także finansowanie działań związanych z wdrożeniem i utrzymaniem systemu łączności radiowej.

Mechanizm finansowania obejmuje jednak wszystkie potrzeby ochrony ludności i obrony cywilnej, co może ograniczać dostępne środki na rozwój systemu łączności, tym bardziej że do zakończenia kontroli nie dokonano oszacowania kosztów wdrożenia systemu. Zarówno Komendant Główny Policji, jak i Komendant Główny PSP nie przedstawili informacji na temat przewidywanych wydatków. Również Minister nie dysponował taką wiedzą (powołany przez niego zespół jest w trakcie szacowania kosztów).

Ponadto opóźnienie we wdrożeniu jednolitego systemu rodzi trudności związane z dotychczasowymi i planowanymi rozwiązaniami poszczególnych służb. Straż Graniczna stosuje inny standard niż planowany system, a Państwowa Straż Pożarna zamierza wdrożyć własne rozwiązanie równoległe do budowy jednolitej sieci. Jednocześnie w przypadku standardu TETRA nierozwiązany pozostaje problem wdrożenia opartego na nim systemu SPR-T w OSP, ponieważ wymaga to uzyskania licencji na użytkowanie algorytmu szyfrującego, przyznawanej wyłącznie organom administracji rządowej oraz jednostkom administracji publicznej. Jednostki OSP, nawet po włączeniu do Krajowego Systemu Ratowniczo-Gaśniczego, nie spełniają tego kryterium, pozostając stowarzyszeniami.

Dodatkowo TETRA, na której ma opierać się system, jest technologią opracowaną w latach 90. i choć nadal jest rozwijana, nie oferuje wszystkich funkcjonalności dostępnych w nowszych systemach. Wymaga to

uwzględnienia perspektywy modernizacji planowanego systemu lub zastąpienia go nowszą technologią w przyszłości. Jednym z jej aspektów powinna być, obok możliwości zarządzania przy pomocy obrazowania w czasie rzeczywistym obszaru objętego działaniami, funkcjonalność umożliwiająca lokalizację sprzętu oraz funkcjonariuszy w trakcie pełnienia służby. Jak pokazują doświadczenia z innych krajów, funkcjonalność tego rodzaju znacznie zwiększa skuteczność wykorzystania sił i środków będących w dyspozycji danej służby. [str. 26–28]

4. WNIOSKI

Wyniki kontroli jednoznacznie wskazują na pilną potrzebę wdrożenia zmian w zakresie organizacji i funkcjonowania systemów łączności radiowej służb podległych Ministrowi Spraw Wewnętrznych i Administracji. Stwierdzone nieprawidłowości, w tym brak jednolitego cyfrowego systemu łączności, niedostateczny nadzór, niedostateczne mechanizmy finansowania oraz problemy z interoperacyjnością – negatywnie wpływają na efektywność współdziałania służb, zwłaszcza w sytuacjach kryzysowych. W związku z tym NIK sformułowała następujące wnioski pokontrolne mające na celu poprawę funkcjonowania łączności radiowej i zwiększenie bezpieczeństwa publicznego, dostrzegając potencjał wynikający z wpisania w 2024 r. zadania utworzenia jednolitego i kompleksowego Systemu Bezpiecznej Łączności Państwowej (SBŁP) do ustawy o ochronie ludności i obronie cywilnej.

**Minister Spraw
Wewnętrznych
i Administracji**

1. Pilne wdrożenie jednolitego systemu cyfrowej łączności radiowej poprzez:
 - a) zapewnienie skutecznej koordynacji i priorytetowego traktowania działań na rzecz budowy Systemu Bezpiecznej Łączności Państwowej (SBŁP), w tym jego podsystemu radiowej łączności trankingowej (SBŁP-T), jako kluczowego elementu zapewnienia bezpieczeństwa i interoperacyjności służb,
 - b) ograniczenie rozwoju niekompatybilnych systemów łączności i zapewnienie spójnego podejścia do budowy infrastruktury radiowej w służbach podległych MSWiA.
2. Opracowanie perspektywicznego modelu działania systemu cyfrowej łączności radiowej uwzględniającego rozwój nowych technologii, w tym m.in. umożliwiających w czasie rzeczywistym lokalizację używanych sił i środków oraz zarządzanie operacjami przy pomocy obrazowania obszaru objętego działaniem, a także integrację z systemami IT, w szczególności w zakresie cyberbezpieczeństwa.
3. Podjęcie przez Ministra SWiA w porozumieniu z ministrem właściwym do spraw informatyzacji skutecznych działań mających na celu włączenia PSP do katalogu podmiotów uprawnionych do korzystania ze świadczenia teleinformatycznego określonego w art. 5 ustawy z dnia 2 grudnia 2021 r. o szczególnych zasadach wynagradzania osób realizujących zadania z zakresu cyberbezpieczeństwa⁶.
4. Wzmocnienie nadzoru nad funkcjonowaniem systemów łączności radiowej w służbach poprzez:

⁶ Dz. U. z 2024 r. poz. 1662.

- a) wprowadzenie mechanizmów systematycznego nadzoru nad funkcjonowaniem i rozwojem systemów łączności radiowej, w tym zapewnienie pełnej informacji o problemach operacyjnych,
 - b) określenie w strukturze MSWiA odpowiedzialnych komórek organizacyjnych nadzorujących łączność radiową i zapewnienie im odpowiednich zasobów kadrowych i kompetencyjnych.
5. Zapewnienie łączności radiowej służbom w budynkach o utrudnionej propagacji sygnału, poprzez przeprowadzenie analizy zasadności stosowania urządzeń retransmisji sygnału, a w razie potrzeby – opracowanie odpowiednich regulacji prawnych.

**Szefowie służb
podległych Ministrowi
SWiA**

- 1. Konsekwentne wycofywanie analogowych systemów łączności niespełniających wymagań bezpieczeństwa i zastąpienie ich – w ścisłym porozumieniu z Ministrem SWiA – nowoczesnymi systemami cyfrowymi zapewniającymi szyfrowanie transmisji.
- 2. Wprowadzenie skutecznych mechanizmów kontroli i nadzoru nad stanem technicznym masztów i instalacji antenowych, zgodnie z przepisami Prawa budowlanego.
- 3. Przygotowanie do przyszłego wdrożenia jednolitego systemu trunkingowej łączności radiowej poprzez opracowanie mechanizmów umożliwiających zapewnienie odpowiedniej liczby wykwalifikowanych specjalistów oraz realizację szkoleń w zakresie wykorzystania takiego systemu oraz zarządzania nim.

5. WAŻNIEJSZE WYNIKI KONTROLI

5.1. BRAK JEDNOLITEGO SYSTEMU ŁĄCZNOŚCI RADIOWEJ DLA SŁUŻB PORZĄDKU I BEZPIECZEŃSTWA WEWNĘTRZNEGO

Podejmowane od wielu lat starania o utworzenie jednolitego ogólnokrajowego systemu łączności radiowej, nie przyniosły dotąd oczekiwanego efektu. Mimo prób oraz prowadzonych prac analityczno-koncepcyjnych, Minister Spraw Wewnętrznych i Administracji nie doprowadził do wdrożenia ogólnokrajowego cyfrowego systemu łączności radiowej dla podległych służb odpowiedzialnych za bezpieczeństwo wewnętrzne i ratownictwo. System ten jest kluczowy dla skutecznego współdziałania funkcjonariuszy, zwłaszcza w sytuacjach kryzysowych, i jest europejskim standardem. Polska wypada niekorzystnie w porównaniu do innych państw europejskich, gdzie podobne systemy zostały wdrożone już wiele lat temu, zapewniając sprawniejsze i bardziej skoordynowane działanie służb w sytuacjach kryzysowych.

5.1.1. DOTYCHCZASOWE DZIAŁANIA NA RZECZ WDROŻENIA JEDNOLITEGO SYSTEMU ŁĄCZNOŚCI RADIOWEJ DLA SŁUŻB MSWiA

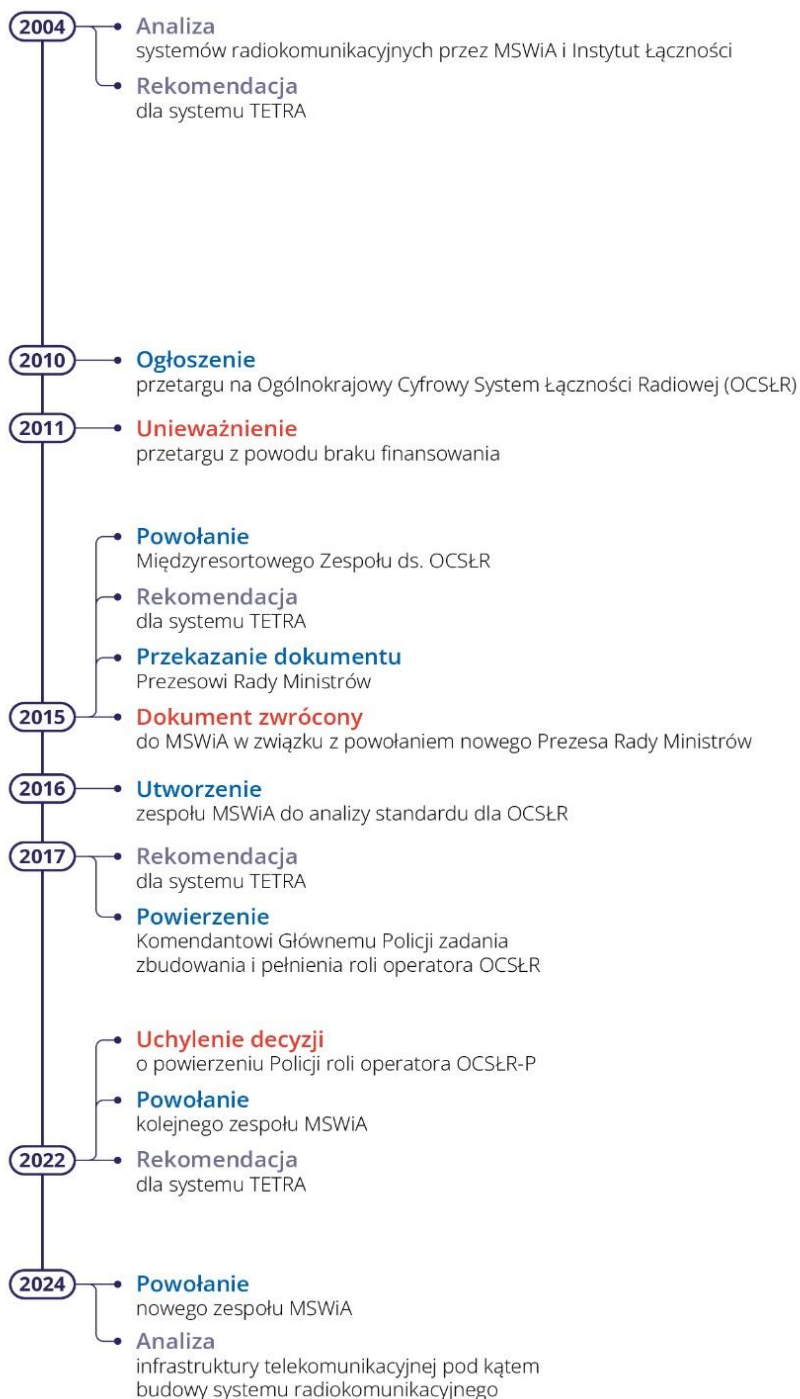
Wieloletnie analizy i kolejne zespoły robocze zamiast wdrożenia systemu

Już w 2004 r. zespół roboczy MSWiA dokonał wraz ze specjalistami z Instytutu Łączności analizy istniejących w Polsce resortowych i specjalnych systemów radiokomunikacyjnych. Wynikało z niej, że istniejące systemy nie spełniają niezbędnych wymagań w zakresie mobilności, trwałości, niezawodności i bezpieczeństwa przekazywanych informacji, a także koordynacji sił i środków w sytuacjach szczególnych – zarówno w skali lokalnej, jak i krajowej – i rekomendowano wprowadzenie systemu trunkingowego opartego na standardzie TETRA. W 2010 r. Centrum Projektów Informatycznych MSWiA ogłosiło przetarg na zaprojektowanie, budowę i wdrożenie Ogólnokrajowego Cyfrowego Systemu Łączności Radiowej dla służb bezpieczeństwa publicznego i ratownictwa na terenie największych miast oraz wybranych powiatów. Projekt miał na celu stworzenie nowoczesnej, bezprzewodowej platformy komunikacyjnej zapewniającej sprawną i bezpieczną wymianę informacji, jednak w 2011 r. został unieważniony z powodu braku możliwości zapewnienia odpowiedniego finansowania tego przedsięwzięcia. Do pomysłu powrócono w 2015 r., kiedy to zarządzeniem Prezesa Rady Ministrów utworzono Międzyresortowy Zespół ds. Ogólnokrajowego

Cyfrowego Systemu Łączności Radiowej⁷, któremu przewodniczył przedstawiciel kierownictwa MSWiA (właściwy w sprawach działalności telekomunikacyjnej).

Infografika nr 2

Działania podejmowane na rzecz utworzenia w Polsce jednolitego systemu cyfrowej łączności radiowej



Źródło: opracowanie własne NIK.

⁷ Zarządzenie nr 67 Prezesa Rady Ministrów z dnia 21 sierpnia 2015 r. w sprawie Międzyresortowego Zespołu do spraw Ogólnokrajowego Cyfrowego Systemu Łączności Radiowej (OCSŁR) (M.P. z 2017 r. poz. 834.). Uchylone z dniem 6 stycznia 2019 r.

**Powtarzane
rekomendacje dla
standardu TETRA**

Do zadań Zespołu należało m.in. dokonanie analizy potrzeb i określenie założeń do budowy OCSŁR, obejmującej w szczególności zakres projektu, technologie, finansowanie oraz harmonogram jego realizacji, a także wypracowanie zasad funkcjonowania systemu oraz określenie zakresu i warunków wykorzystania OCSŁR przez organy administracji rządowej oraz jednostki organizacyjne im podległe lub przez nie nadzorowane.

Wypracowane przez Zespół wnioski i rekomendacje zostały przekazane do akceptacji ówczesnego Prezesa Rady Ministrów 9 listopada 2015 r. W dokumencie po raz kolejny stwierdzono konieczność stworzenia wspólnego systemu łączności radiowej opartego na technologii TETRA, który umożliwiłby niezawodną łączność na dowolnym obszarze kraju dla podmiotów działających w obszarze bezpieczeństwa publicznego i ratownictwa, w tym Policji, Państwowej Straży Pożarnej, Straży Granicznej, Państwowego Ratownictwa Medycznego, Agencji Bezpieczeństwa Wewnętrznego oraz wojewodów. Dokument ten jednakże został zwrócony przez Kancelarię Prezesa Rady Ministrów do MSWiA w związku z powołaniem w 2015 r. nowego Prezesa Rady Ministrów. Tym samym istotne zadanie państwa w zakresie zbudowania systemu bezpiecznej łączności służb podległych MSWiA nie zostało zrealizowane.

W tej sytuacji W 2016 r. Minister SWiA powołał własny zespół do przeprowadzenia analizy w zakresie wyboru standardu dla Ogólnokrajowego Cyfrowego Systemu Łączności Radiowej, który w styczniu 2017 r. przedstawił wyniki wraz z kolejną rekomendacją wdrożenia systemu w oparciu o technologię cyfrową w standardzie TETRA, bazując na istniejącej i planowanej do rozbudowy infrastrukturze Policji. Zaakceptowana przez ówczesnego Ministra SWiA w czerwcu 2017 r. notatka służbowa dotycząca budowy i wdrożenia Ogólnokrajowego Cyfrowego Systemu Łączności Radiowej w oparciu o infrastrukturę TETRA Policji – system „OCSŁR-P” zawierała m.in. wniosek, że system ten powinien zostać przeznaczony dla służb podległych i nadzorowanych przez Ministra, z uwzględnieniem możliwości jego udostępnienia na poziomie systemowym innym użytkownikom, realizującym zadania z obszaru bezpieczeństwa i porządku publicznego oraz ratownictwa. Minister powierzył Komendantowi Głównemu Policji zadanie zbudowania jednolitego systemu cyfrowej łączności radiowej struktur zarządzania kryzysowego i służb ratowniczych oraz rolę jego operatora. Policja została wybrana ze względu na swój potencjał, doświadczenie w modernizacji sieci radiowych oraz skuteczne wdrożenie systemu TETRA w czterech miastach. Z różnych powodów (więcej w p. 5.1.2) nie udało się jednak zrealizować tego przedsięwzięcia. Minister Spraw Wewnętrznych i Administracji Decyzją nr 31 z 8 sierpnia 2022 r. uchylił decyzję w sprawie powierzenia Komendantowi Głównemu Policji zadań operatora OCSŁR-P, uzasadniając to m.in. względami finansowymi.

W sierpniu 2022 r. w MSWiA utworzono następny Zespół, którego zadaniem było dokonanie analizy dostępnych technologii łączności radiowej i przedstawienie rekomendacji do wdrożenia cyfrowego systemu radiokomunikacyjnego dla potrzeb organów i jednostek organizacyjnych w resorcie spraw wewnętrznych. W jego skład wchodził przedstawiciel m.in. Policji, Państwowej Straży Pożarnej, Służby Ochrony Państwa oraz Departamentu Teleinformatyki (dalej: DT) MSWiA. Do zadań zespołu należało przeprowadzenie analizy cyfrowych systemów łączności radiowej oraz opracowanie zaleceń do wdrożenia cyfrowego systemu radiokomunikacyjnego dla ww. podmiotów. Zespół w przedstawionej Ministrowi analizie zarekomendował wdrożenie CSR w oparciu o technologię cyfrową w standardzie TETRA z szyfrowaniem interfejsu radiowego w standardzie TEA2, z uwzględnieniem możliwie szerokiego stosowania szyfrowania pomiędzy urządzeniami końcowymi, tzw. „end to end”, poprzez rozszerzenie obszarowe budowanej przez Policję platformy radiokomunikacyjnej dla służb pionu kontrterrorystycznego oraz pozostałych jednostek i komórek organizacyjnych Policji, pod warunkiem jej przeznaczenia do realizacji potrzeb służb podległych MSWiA. Ponadto przewidziano możliwość udostępnienia przedmiotowej technologii dla innych podmiotów realizujących zadania z obszaru bezpieczeństwa, porządku publicznego, ratownictwa i zarządzania kryzysowego na obszarze kraju.

Kolejny zespół powołany przez Ministra w lipcu 2024 r. otrzymał zadanie przeprowadzenia analizy możliwości wykorzystania infrastruktury telekomunikacyjnej na potrzeby budowy i wdrożenia cyfrowego systemu radiokomunikacyjnego oraz opracowania koncepcji wdrożenia tego systemu, a następnie przedstawienie jej wyników w terminie sześciu miesięcy.

Pomimo tych inicjatyw, pełne wdrożenie jednolitego, trankingowego systemu łączności radiowej dla służb podległych MSWiA nadal pozostaje w fazie planowania i realizacji.

5.1.2. NIEPOWODZENIE PRZEDSIĘWZIĘCIA BUDOWY OGÓLNOKRAJOWEGO CYFROWEGO SYSTEMU ŁĄCZNOŚCI RADIOWEJ

Powierzenie przez Ministra SWiA Komendantowi Głównemu Policji zadania zbudowania jednolitego systemu cyfrowej łączności radiowej struktur zarządzania kryzysowego i służb ratowniczych⁸ oraz roli jego operatora odbyło się w oparciu o środki z „Programu modernizacji Policji, Straży Granicznej, Państwowej Straży Pożarnej i Służby Ochrony Państwa w latach 2017–2020”. Policja miała zmodernizować w pierwszym etapie

⁸ Decyzja nr 164 Ministra SWiA z dnia 31 lipca 2017 r.

Brak narzędzi do skutecznego wdrożenia systemu

swoje sieci radiowe na obszarze 13 miast wojewódzkich, a następnie udostępnić je do wykorzystywania innym służbom. Służbie tej nie udało się jednak przeprowadzić skutecznie postępowań przetargowych na zakup niezbędnego sprzętu, co doprowadziło do niepowodzenia przedsięwzięcia. Umowa zawarta z dostawcą sprzętu w wyniku drugiego z postępowań (pierwsze pozostało nierozstrzygnięte) została unieważniona w 2020 r. na podstawie decyzji Krajowej Izby Odwoławczej (KIO), której prawidłowość potwierdził Sąd Okręgowy w Warszawie. Przyczyną takiej decyzji było udzielenie przez Policję zamówienia w trybie z wolnej ręki jednemu producentowi, co skutkowało złożeniem odwołania do KIO przez pozostałych oferentów. KIO uznała ich zarzuty za zasadne.

Na podstawie analizy doświadczeń Policji we wdrażaniu OCSŁR-P NIK zidentyfikowała trzy problemy, które zdecydowały o niepowodzeniu przedsięwzięcia. Po pierwsze, inicjatywa oraz koordynacja budowy systemu przeznaczonego dla ogółu służb i instytucji państwowych na terenie całego kraju została powierzona Komendantowi Głównemu Policji, podczas gdy powinna być podjęta na wyższym poziomie, nawet gdyby konkretne prace lub zadania w ramach takiego projektu były zlecone wybranej służbie. Wymaga to bowiem skoordynowania potrzeb wielu podmiotów, co wykracza poza kompetencje jednej formacji. Budowa systemu ogólnokrajowego to przedsięwzięcie strategiczne, jednak nie było ono prowadzone na poziomie rządu lub dedykowanego organu państwowego. Brak takiej koordynacji nie gwarantował niezbędnych zasobów, właściwych priorytetów oraz odporności na zagrożenia cybernetyczne, sabotaż i sytuacje kryzysowe.

Po drugie, z ustaleń kontroli wynika, że najistotniejszą z przyczyn porażki wdrożenia jednolitego systemu łączności radiowej był brak dedykowanego dla tego zadania mechanizmu finansowania. Jedynie dwóm najmniejszym służbom udało się wdrożyć samodzielnie cyfrowe systemy łączności (SOP i Straż Graniczna) w oparciu o własne budżety i programy modernizacyjne. Natomiast Policja na podstawie doświadczeń zgromadzonych podczas próby wdrożenia OCSŁR-P uznała za niezbędne wprowadzenie dedykowanego mechanizmu finansowania, który zapewni skuteczną realizację podobnego zadania w przyszłości. Kiedy finansowanie budowy systemu OCSŁR-P wygasło z końcem obowiązywania wyżej wymienionego Programu Modernizacji, Minister Spraw Wewnętrznych i Administracji Decyzją nr 31 z 8 sierpnia 2022 r. uchylił decyzję w sprawie powierzenia Komendantowi Głównemu Policji zadań operatora OCSŁR-P. Uzasadnił to m.in. właśnie względami finansowymi.

Ryzyka związane z przetargami

Po trzecie, niepowodzenie oraz zebrane doświadczenie skłoniły Policję do opinii, że wybór wykonawcy powinien być realizowany poza reżimem

ustawy Prawo Zamówień Publicznych (analogiczne rozwiązania przyjęte są np. w Siłach Zbrojnych RP) i na poziomie państwowym, a nie wyłącznie przez jedną ze służb. Rozwiązanie to mogłoby przyczynić się do przyspieszenia realizacji projektu oraz zwiększenia jego bezpieczeństwa operacyjnego. Umożliwiłoby lepszą kontrolę nad jakością (wybór dostawcy na podstawie doświadczenia i oceny technologii) oraz zwiększone bezpieczeństwo i poufność (poprzez uniknięcie ryzyka ujawnienia wrażliwych informacji o systemie w publicznych postępowaniach przetargowych). Rozwiązanie to nie jest jednak pozbawione ryzyk, w tym ograniczenia konkurencyjności, wzrostu kosztów oraz potencjalnych nieprawidłowości w procesie wyboru wykonawcy (np. faworyzowania konkretnych podmiotów). W związku z tym jego przyjęcie wymagałoby zastosowania dodatkowych mechanizmów nadzoru i kontroli w celu minimalizacji zagrożeń oraz zapewnienia transparentności i efektywności wydatkowania środków publicznych. Niezależnie od przyjętego podejścia, proces udzielania zamówień publicznych w ramach budowy jednolitego systemu łączności wiąże się z istotnymi ryzykami, które wymagają odpowiedniego zarządzania.

W celu przezwyciężenia opisanych wyżej trudności Zastępca Komendanta Głównego Policji w styczniu 2024 r. zwrócił się do Ministra Spraw Wewnętrznych i Administracji w sprawie zainicjowania, na poziomie ministerstwa, działań zmierzających do włączenia do budowanego Systemu Radiokomunikacyjnego Policji – TETRA organizacji służb państwowych innych niż Policja i jednoczesnego uregulowania zasad finansowania i utrzymania tego systemu. Propozycja Komendanta jest przedmiotem analizy w kontekście planowanego systemu bezpiecznej, szyfrowanej łączności państwowej.

5.1.3. PERSPEKTYWY WDROŻENIA JEDNOLITEGO SYSTEMU ŁĄCZNOŚCI W ŚWIEŁIE USTAWY O OCHRONIE LUDNOŚCI I OBRONIE CYWILNEJ

M.in. w odpowiedzi na ponawiane wnioski NIK – postulujące wprowadzenie jednolitego systemu cyfrowej łączności radiowej struktur zarządzania kryzysowego i służb ratowniczych na terenie kraju (sformułowane po kontrolach: P/17/019 *Ochrona ludności w ramach zarządzania kryzysowego i obrony cywilnej*⁹ oraz P/22/029 *Przygotowanie państwa na zagrożenia związane z działaniami hybrydowymi*¹⁰) – Minister podjął działania ustawodawcze w celu ich realizacji. Inicjatywa ta dotyczyła opracowania projektu ustawy o ochronie ludności i obronie cywilnej, obejmującego m.in. utworzenie systemu bezpiecznej łączności państwowej, który – po uzgodnieniach i konsultacjach – 18 września

⁹ Zob.: <https://www.nik.gov.pl/kontrole/P/17/039/>

¹⁰ Zob.: <https://www.nik.gov.pl/kontrole/P/22/029/>

**Ustawa solidną
podstawą dla
wdrożenia jednolitego
systemu łączności**

2024 r. został skierowany do Sejmu RP. W wyniku prac legislacyjnych ustawę uchwalono na posiedzeniu w dniu 5 grudnia 2024 r., a Prezydent RP podpisał ją w dniu 17 grudnia 2024 r.¹¹ Opisany w ww. ustawie System Bezpiecznej Łączności Radiowej ma zapewnić ciągłość funkcjonowania administracji państwowej oraz ochrony ludności na czas pokoju i wojny, a jednym z jego podsystemów będzie system bezpiecznej radiowej łączności trunkingowej (SBŁP-T), stanowiący jednolity system cyfrowej łączności radiowej struktur zarządzania kryzysowego i służb ratowniczych.

Ustawa o ochronie ludności i obronie cywilnej wprowadza rozwiązania, które na poziomie regulacji niwelują kluczowe bariery uniemożliwiające dotychczas wdrożenie jednolitego, ogólnokrajowego systemu łączności radiowej. Przepisy ustawy określają zasady organizacji, finansowania i nadzoru nad wdrożeniem i utrzymaniem systemu. Stanowi to istotny krok w kierunku stworzenia nowoczesnej, bezpiecznej infrastruktury łączności, niezbędnej do skutecznego działania służb w sytuacjach kryzysowych.

Zgodnie z art. 74 ww. ustawy Minister SWiA jest odpowiedzialny za organizację i nadzór nad SBŁP i pełni rolę operatora tego systemu. Jako operator ma zapewnić:

- zbudowanie interoperacyjności między systemami łączności i komunikacji administracji publicznej, służb podległych ministrowi właściwemu do spraw wewnętrznych oraz innymi wydzielonymi systemami łączności, w tym z systemami pozostającymi we właściwości Ministra Obrony Narodowej,
- możliwość przekazywania informacji o zagrożeniach między elementami systemu wykrywania zagrożeń,
- możliwość powiadamiania, ostrzegania i alarmowania ludności o zagrożeniach oraz zapewnienia bezpiecznej łączności między służbami państwowymi oraz podmiotami ochrony ludności przy wykonywaniu zadań ochrony ludności i ochrony porządku publicznego,
- funkcjonowanie kanałów łączności w sieciach telekomunikacyjnych, z uwzględnieniem sieci stacjonarnej, radiowej, komórkowej i satelitarnej.

Zgodnie z art. 81 ustawy Prezes Rady Ministrów na wniosek ministra właściwego do spraw wewnętrznych, uzgodniony z Ministrem Obrony Narodowej, w drodze zarządzenia, powołuje Pełnomocnika Rządu ds. Systemu Bezpiecznej Łączności Państwowej (SBŁP) i określa jego szczegółowy zakres działania. Ponadto w ustawie przewidziano wydanie

¹¹ Dz. U. poz. 1907

dwóch rozporządzeń w zakresie sposobu udziału służb i innych podmiotów w budowie, utrzymaniu i rozwoju SBŁP oraz szczegółowych warunków świadczenia usług telekomunikacyjnych w ramach systemu, a także sposobu korzystania z SBŁP przez użytkowników, minimalnych wymagań technicznych i funkcjonalnych oraz minimalnego poziomu bezpieczeństwa systemu, mając na względzie konieczność zapewnienia odpowiedniego poziomu bezpieczeństwa komunikacji. Obowiązki te, określone w art. 76 ust. 5 i art. 78 ust. 2, wchodzi w życie po upływie roku od dnia ogłoszenia, tj. od 24 grudnia 2025 r.

Przyjęto, że sposób finansowania realizacji zadań w powyższym zakresie określa Program Ochrony Ludności i Obrony Cywilnej, opracowywany na okres czterech lat i aktualizowany co dwa lata. Pierwszy program ma zostać opracowany w terminie trzech miesięcy od dnia ogłoszenia ustawy i będzie stanowił podstawę finansowania realizacji zadań ochrony ludności i obrony cywilnej w latach 2025–2026. Ustawa określa, że na ten cel przeznaczają się corocznie środki będące w dyspozycji m.in. Ministra SWiA oraz Ministra Obrony Narodowej, w wysokości nie niższej niż 0,3 proc. PKB (produktu krajowego brutto)¹².

Przyjęte rozwiązania prowadzą do jasnego określenia ról i podziału zadań, przenoszą ich koordynację na poziom centralny oraz zapewniają stały mechanizm finansowania. Mechanizm ten obejmuje jednak wszystkie potrzeby ochrony ludności i obrony cywilnej, co może ograniczać dostępne środki na rozwój systemu łączności. Przykładowo potrzeby w zakresie budowy schronów dla ludności są w naszym kraju ogromne. Aby zapewnić skuteczne wdrożenie jednolitego systemu łączności radiowej, konieczne będzie priorytetowe traktowanie jego finansowania w ramach dostępnych środków lub rozważenie wyodrębnienia dedykowanego mechanizmu budżetowego, tak aby nie konkutował on z innymi kluczowymi zadaniami w zakresie ochrony ludności.

**Zagrożenia wynikające
z wieloletnich
opóźnień**

Do zakończenia czynności kontrolnych nie były znane koszty wdrożenia systemu. W zatwierdzonej w grudniu 2022 r. „Analizie dostępnych technologii wraz z rekomendacją kierunkową do wdrożenia cyfrowego systemu radiokomunikacyjnego”, nie określono przewidywanych kosztów wdrożenia CSR w oparciu o rekomendowany system TETRA. Powyższe zadanie zostało powierzone przez Ministra w lipcu 2024 r. Zespołowi do przeprowadzenia analizy możliwości wykorzystania infrastruktury telekomunikacyjnej, który został zobowiązany do przygotowania

¹² W terminie 60 dni od dnia zatwierdzenia pierwszego Programu Ochrony Ludności i Obrony Cywilnej Minister Finansów, na zgodny wniosek Ministra SWiA i Ministra Obrony Narodowej, dokona przeniesień wydatków zaplanowanych w dziale „obrona narodowa” między częściami budżetu państwa.

propozycji w zakresie mechanizmów i źródeł finansowania utrzymania i rozbudowy CSR.

Ponadto wprowadzenie jednolitego systemu będzie obecnie trudniejsze, ponieważ służby już zainwestowały w inne rozwiązania lub planują systemy w innym standardzie. Straż Graniczna o SOP stosują odmienne standardy niż przyjęty w zapowiadzianym systemie, a Państwowa Straż Pożarna zamierza wdrożyć własne rozwiązanie równoległe do budowy jednolitej sieci (więcej w p. 5.2). Dodatkowo technologia TETRA, na której ma opierać się system, jest technologią opracowaną w latach 90. i choć nadal jest rozwijana, nie oferuje wszystkich funkcjonalności dostępnych w nowszych systemach. Wymaga to uwzględnienia perspektywy modernizacji planowanego systemu lub zastąpienia go nowszą technologią w przyszłości.

Mimo to w opinii Instytutu Łączności PIB¹³ – wyrażonej na gruncie doświadczeń związanych ze współpracą z firmami energetycznymi zainteresowanymi rozwiązaniami radiokomunikacyjnymi – systemy trunkingowe oparte na standardzie TETRA pozostają niezawodnym i skutecznym rozwiązaniem łączności dedykowanym do stosowania dla celów zapewnienia bezpieczeństwa publicznego, w tym w nadzwyczajnych okolicznościach związanych z sytuacjami kryzysowymi wynikającymi z przyczyn naturalnych. Kluczowe będzie w tym przypadku zapewnienie bezpiecznej i dobrze pod względem technicznym zaprojektowanej infrastruktury (w tym zapewnienie podtrzymania baterijnego) oraz mechanizmów bezpiecznego i pozostającego pod właściwą kontrolą zarządzania całością sieci i usług.

W opinii NIK należy także śledzić rozwój standardów, które umożliwiają integrację tradycyjnych systemów radiowych z nowoczesnymi sieciami. Uwzględnienie tych standardów w projektowanej sieci radiokomunikacyjnej ułatwi przejście służb na bardziej zaawansowaną infrastrukturę. Konieczna jest przy tym analiza takich wdrożeń na świecie, aby zidentyfikować najlepsze praktyki i ocenić możliwości ich adaptacji do polskich warunków (więcej o tym na str. 44–45).

5.2. FUNKCJONOWANIE SYSTEMÓW ŁĄCZNOŚCI RADIOWEJ W POSZCZEGÓLNYCH SŁUŻBACH

Służby autonomicznie rozwijały systemy łączności

Z uwagi na brak jednolitego cyfrowego systemu łączności radiowej poszczególne służby rozwijały własne rozwiązania, kierując się przede wszystkim indywidualnymi potrzebami i możliwościami. Łączne koszty

¹³ Przekazanej NIK przez Instytut Łączności PIB w dn. 22 stycznia 2025 r.

poniesione przez nie na łączność radiową w latach 2016–2023 (w SG od 2011 r.) wyniosły blisko 435 mln zł.

W dalszej części informacji przedstawione zostaną rozwiązania przyjęte w poszczególnych służbach. Nie będzie to szczegółowa prezentacja aspektów technicznych, z którymi zapoznali się kontrolerzy, lecz przedstawienie ich kluczowych aspektów. Celem omówienia jest przede wszystkim ocena możliwości skutecznej realizacji zadań przez służby oraz analiza uwarunkowań istotnych z perspektywy planowanej budowy jednolitego systemu łączności radiowej.

5.2.1. POLICJA

W okresie objętym kontrolą Policja wykorzystywała cztery standardy łączności.

**Podstawowym
systemem łączności
Policji pozostawał
system analogowy**

1. W 2024 r. – pomimo formalnego wprowadzenia dwa lata wcześniej systemu SRP-T jako głównego systemu tej służby – podstawowym systemem Policji pozostawał system analogowy. Był podstawowym systemem łączności radiowej w 14 Komendach Wojewódzkich Policji (82,4 proc.) i w 201 Komendach Powiatowych (miejskich) Policji (58,6 proc.)¹⁴. W oparciu o rozwiązanie analogowe funkcjonowała także sieć współdziałania KSWA¹⁵;
2. Cyfrowy system TETRA wdrożony został w 2014 r. w Łodzi oraz w 2017 r. w Krakowie, Szczecinie oraz Warszawie. Jego ulepszona wersja wprowadzona została do użytkowania w Centralnym Pododdziale Kontrterrorystycznym Policji „BOA” oraz w komórkach kontrterrorystycznych działających przy wszystkich KWP/KSP w kraju¹⁶. Ponadto system TETRA w postaci stałych stacji bazowych (na różnych poziomach wdrożenia) był dostępny na obszarach odpowiedzialności: Komendy Stołecznej Policji oraz KWP w Bydgoszczy, Gdańsku, Gorzowie Wielkopolskim, Kielcach, Krakowie, Łodzi, Poznaniu, Rzeszowie, Szczecinie, Wrocławiu. W 2022 r. System Radiokomunikacyjny Policji – TETRA (SRP-T) został formalnie wdrożony do eksploatacji, a jego rozwój jest kontynuowany w miarę możliwości finansowych formacji.
3. W celu zniwelowania problemów wynikających z użytkowania przestarzałej technologii analogowej, w części jednostek wprowadzono otwarty standard cyfrowej łączności radiowej DMR

¹⁴ Dane na dzień 5 grudnia 2024 r.

¹⁵ Krajowa Sieć Współdziałania i Alarmowania – sieć radiowa pracująca na ogólnopolskim kanale radiowym i wykorzystywana w razie zaistnienia odpowiednich okoliczności do wywołania, powiadamiania i współdziałania stacji stałej z dowolną inną stacją znajdującą się w jej zasięgu.

¹⁶ W 2024 r. podwyższenie standardu objęło całość systemu TETRA w Policji.

(Digital Mobile Radio). Urządzenia abonenckie (radiotelefony) DMR były użytkowane przez KGP oraz przez wszystkie KWP/KSP w kraju. Rozwój technologii DMR został częściowo wstrzymany przez decyzję KGP o rozwoju systemu cyfrowego TETRA. Przykładowo w KWP zs. w Radomiu, na terenie której w 24 komendach miejskich i powiatowych wykorzystywano do komunikacji analogowy system łączności radiowej, a w czterech komendach powiatowych cyfrowy w standardzie DMR, wstrzymane zostało dalsze wdrażanie tego standardu z powodu planu rozwoju systemu cyfrowego TETRA.

4. Technologia EDACS (Enhanced Digital Access Communication System) była wykorzystywana w Policji od 1995 r. w formie rozwiązań wyspowych oferujących zasięg na ograniczonym obszarze, a nie w formie jednolitego, ogólnokrajowego systemu. EDACS służył do wewnętrznej łączności Policji o charakterze lokalnym. Jednostki szczebla wojewódzkiego decydowały o zasadności i sposobie jego wykorzystania. W praktyce został wycofany z eksploatacji. Powodem było zacofanie technologiczne, trudność w pozyskiwaniu części zamiennych oraz brak natywnego wsparcia dla szyfrowania połączeń, które możliwe było jedynie dzięki dodatkowym komponentom.

Przykład

Zacofanie technologiczne systemu EDACS wykazane zostało przez dziennikarzy, którzy 3 maja 2019 r. udokumentowali nieautoryzowane przechwycenie komunikacji radiowej Policji ochraniającej najważniejsze osoby w państwie. Do przechwycenia transmisji wykorzystano ogólnodostępne skanery radiowe warte kilkaset złotych. Umożliwiło to osobom postronnym uzyskanie dostępu do treści rozmów operacyjnych funkcjonariuszy. Konsekwencją tego incydentu było ujawnienie procedur działania służb oraz potencjalne zagrożenie dla bezpieczeństwa ochranianych osób.

Zastąpienie systemu EDACS standardem TETRA w praktyce uniemożliwiło przechwytywanie komunikacji Policji tam, gdzie standard ten został wdrożony. Problemem pozostawała jednak wielość przyjętych rozwiązań radiowych. Aby zapewnić spójną komunikację radiową wykorzystywane były interfejsy radiowe, które umożliwiały zespolenie grup radiowych TETRA i DMR. Przykładowo interfejsy takie działały na wyznaczonych stanowiskach, np. na Stołecznym Stanowisku Kierowania. Były także instalowane w wybranych miejscach w garnizonie warszawskim, dzięki czemu możliwe było wcześniejsze zaplanowanie i zestawienie grup łączących funkcjonariuszy komunikujących się w DMR i TETRA (np.

w przypadku działania grup policyjnych zajmujących się zwalczaniem przestępczości samochodowej, działających często na styku miasta stołecznego i okolicznych powiatów). Ich zastosowanie pozostawało jednak ograniczone, więc warszawscy policjanci byli instruowani, by w sytuacji wykonywania zadań na terenie rozszerzonym, tj. objętym przez system TETRA i DMR, wyposażali się w dwa radiotelefony. W przypadku realizacji zadań przez funkcjonariuszy na obszarze funkcjonowania sieci konwencjonalnej (analogowej), do nawiązania łączności radiowej wykorzystywana była dodatkowo Krajowa Sieć Współdziałania i Alarmowania. W tej policyjnej sieci o zasięgu krajowym funkcjonariusze mieli możliwość nawiązania kontaktu z dyżurnymi jednostek, na których obszarze się znajdowali. Pomimo tych starań wielość wykorzystywanych systemów łączności sprawiała, że policjanci, szczególnie w sytuacjach dynamicznych, mogli napotkać na problemy związane z brakiem jednolitego systemu łączności.

**Policyjny system
łączności wymagał
utrzymywania
dodatkowego sprzętu**

Ograniczenia policyjnego systemu łączności radiowej uwidaczniały się także w sytuacjach wymagających masowych zabezpieczeń, charakterystycznych dla większych miast. Realizacja takich działań często wiązała się z koniecznością pozyskania wsparcia spoza miejscowego garnizonu. Przykładowo w stolicy w takich sytuacjach funkcjonariusze spoza właściwego garnizonu byli doposażani w radiotelefony ze stanu Komendy Stołecznej Policji. To wiązało się z koniecznością utrzymywania wysokiej liczby redundantnych radiotelefonów. Możliwe było również rozwiązanie polegające na wydzieleniu konwencjonalnego kanału simpleksowego, na którym przyjezdni funkcjonariusze mogli prowadzić korespondencję na własnych radiotelefonach. Rozwiązanie takie uniemożliwiało jednak bezpośrednie porozumiewanie się między policjantami z garnizonu stołecznego i spoza niego (tj. tych, którzy używali łączności konwencjonalnej i łączności TETRA). W tej sytuacji komunikacja odbywała się poprzez łączników wyposażonych w dwa radiotelefony.

Od 2022 r. Policja wdraża System Radiokomunikacyjny Policji – Tetra (SRP-T). Wdrożenie ma charakter rozwoju istniejącego systemu i zależne jest od pozyskanych z roku na rok funduszy. Realizowane jest w miarę posiadanych możliwości finansowych i kadrowych w samej KGP, jak i w jednostkach szczebla KWP/KSP realizujących lokalnie rozbudowę w formie własnych projektów teleinformatycznych. Z tego powodu Policja nie oszacowała całościowo kosztów wdrożenia systemu. Wszystko to sprawia, że niemożliwe jest dokładne określenie, kiedy zostanie on uruchomiony w całym kraju.

5.2.2. PAŃSTWOWA STRAŻ POŻARNA

Funkcjonujący w PSP analogowy system łączności radiowej nie spełniał wymagań stawianych służbom ratowniczym i porządku publicznego w zakresie poufności korespondencji, bezpieczeństwa danych, jakości połączeń oraz utrudniał efektywną organizację łączności. System łączności PSP nie pozwalał również (poza wyjątkami związanymi z czasowym użytkowaniem systemu TETRA na terenie wybranych miast) na efektywną i bezpieczną komunikację ze służbami podległymi MSWiA, a także innymi podmiotami realizującymi zadania zarządzania kryzysowego oraz obronności państwa.

Dominacja systemu analogowego w PSP

W Komendzie Głównej Państwowej Straży Pożarnej i jednostkach podległych co do zasady funkcjonowały konwencjonalne analogowe systemy łączności radiowej oparte o UKF. Nie umożliwiały one transmisji danych, a ich podstawowe wykorzystanie polegało na zapewnieniu nieszyfrowanej komunikacji głosowej. W związku z tym stosowane były kryptonimy oraz formalnie określone sygnały radiowe, a ochrona poufności komunikacji opierała się głównie na zasadach formalnych, które polegały na zakazie przekazywania określonych informacji (imion, nazwisk, stopni służbowych) w otwartych transmisjach. Dodatkowo PSP wykorzystywała pojedyncze funkcjonujące lokalnie cyfrowe systemy łączności radiowej TETRA lub DMR.

Podczas korzystania z systemów łączności przez funkcjonariuszy Państwowej Straży Pożarnej – w związku z dominacją sieci analogowej – występowały trudności związane z ograniczonym zasięgiem fal radiowych, zakłóceniami wynikającymi z nadmiernej liczby użytkowników na wspólnym kanale oraz brakiem szyfrowania. Dodatkowo, technologia analogowa nie wspierała zaawansowanych funkcji, takich jak transmisja danych czy lokalizacja GPS. Problematiczna była także interoperacyjność pomiędzy różnymi systemami komunikacyjnymi wykorzystywanymi przez służby (np. TETRA i systemy analogowe), co wymagało dodatkowych narzędzi integracyjnych. Na jakość łączności wpływały również warunki terenowe i atmosferyczne, powodujące przerwy w komunikacji.

System analogowy powodował w PSP liczne trudności

Funkcjonariusze PSP zwracali także uwagę na istotne trudności w zapewnieniu skutecznej łączności radiowej w obiektach o specyficznej architekturze, w których występuje efekt tzw. klatki Faradaya, uniemożliwiający efektywną propagację fal radiowych. Ograniczenia te mogą znacząco utrudniać koordynację działań ratowniczych oraz komunikację funkcjonariuszy Państwowej Straży Pożarnej w sytuacjach kryzysowych. Problemy te nie występują w budynkach, gdzie wdrożono systemy retransmisji sygnału radiowego dedykowane służbom ratunkowym, co wskazuje na skuteczność tego rozwiązania w eliminowaniu zakłóceń. W celu zapewnienia ciągłości łączności PSP

musiała stosować alternatywne sposoby komunikacji, w tym oparte na cywilnej sieci LTE. Zidentyfikowano przy tym brak regulacji prawnych dotyczących obowiązku stosowania odpowiednich urządzeń i rozwiązań technicznych w budynkach o utrudnionej propagacji sygnału. Brak jednolitych wytycznych w tym zakresie może prowadzić do sytuacji, w której w niektórych obiektach, zwłaszcza nowoczesnych budowlach o konstrukcji ograniczającej przenikanie fal radiowych, skuteczna komunikacja będzie niemożliwa.

Problemy wynikające z wykorzystywania sieci analogowej przy jednoczesnym braku jednolitego krajowego systemu łączności radiowej dla służb sprawiły, że Państwowa Straż Pożarna podjęła decyzję o wdrożeniu standardu DMR. W celu opracowania strategii migracji do systemu cyfrowego oraz określenia wymagań technicznych Komendant Główny PSP w grudniu 2022 r. powołał zespół zadaniowy, który w dniu 9 stycznia 2024 r. przedstawił szczegółową *Koncepcję migracji na cyfrową łączność radiową DMR w PSP*. Dokument ten zawierał kompleksowy opis stanu obecnego sieci radiowych, priorytetów PSP w zakresie cyfryzacji łączności, a także szczegółowe wymagania techniczno-funkcjonalne dla systemu radiowego. Decyzja o wdrożeniu standardu DMR w Państwowej Straży Pożarnej została podjęta z konieczności zapewnienia niezawodnej i bezpiecznej komunikacji, która sprostą wymaganiom zarówno PSP, jak i Ochotniczych Straży Pożarnych. Wybór standardu DMR został przez PSP uzasadniony możliwością zwiększenia zasięgu transmisji oraz poprawą jakości przekazu głosowego, co jest kluczowe dla efektywnej koordynacji działań ratowniczych. Ponadto DMR ma umożliwić integrację jednostek OSP w ramach Krajowego Systemu Ratowniczo-Gaśniczego, co znacząco podniesie elastyczność i skalowalność systemu łączności.

Dwie rozbieżne koncepcje łączności dla PSP

Przyjęcie przez Państwową Straż Pożarną koncepcji migracji na cyfrową łączność radiową w standardzie DMR stało jednak w sprzeczności z założeniami opracowanymi na szczeblu ministerialnym. W grudniu 2022 r. Zespół powołany przez Ministra Spraw Wewnętrznych i Administracji, w którego skład wchodził również przedstawiciel PSP, opracował *Analizę dostępnych technologii wraz z rekomendacją kierunkową do wdrożenia cyfrowego systemu radiokomunikacyjnego dla potrzeb organów i jednostek organizacyjnych podległych ministrowi właściwemu do spraw wewnętrznych lub przez niego nadzorowanych*. Dokument ten wskazywał jako docelowe rozwiązanie wdrożenie jednolitego Cyfrowego Systemu Radiokomunikacyjnego (CSR) w technologii TETRA, poprzez rozbudowę istniejącej infrastruktury policyjnej SRP-T i przekształcenie jej w platformę ogólnokrajową przeznaczoną dla wszystkich służb resortu. Wskazano, że w perspektywie kilku lat system ten mógłby objąć cały kraj, co zapewniłoby jednolitą i interoperacyjną łączność. W analizie jednoznacznie uznano standard DMR za nieperspektywny w kontekście budowy

**Problem z włączeniem
OSP do systemu TETRA**

ogólnokrajowego systemu łączności dla służb. Argumentowano to m.in. brakiem istotnych wdrożeń w Europie, ograniczonymi możliwościami integracji z systemami państw sąsiadujących oraz niedoborem dostępnych częstotliwości.

W związku z tym decyzja PSP o wdrożeniu DMR, oparta na autonomicznych przesłankach, odbiegała od rekomendacji MSWiA i kierunku planowanego rozwoju systemów łączności dla służb podległych resortowi. Miała jednak na celu stosunkowo szybkie przewyższenie ograniczeń wynikających z użytkowania sieci analogowych, charakteryzujących się ograniczonym zasięgiem i podatnością na zakłócenia, nie zapewniających spójnej łączności, szczególnie w warunkach terenowych i podczas masowych zabezpieczeń, gdzie niezbędne jest wsparcie jednostek z różnych regionów. Dodatkowo w przypadku standardu TETRA nierozwiązany pozostaje problem wdrożenia takiego systemu w OSP. Włączenie podmiotów do systemu TETRA SPR-T napotyka na ograniczenia wynikające z wymogu posiadania licencji na użytkowanie algorytmu szyfrującego, która jest udzielana wyłącznie organom administracji rządowej oraz jednostkom administracji publicznej odpowiedzialnym za zadania związane z ochroną bezpieczeństwa, porządku publicznego, ratownictwem i zarządzaniem kryzysowym. W praktyce oznacza to, że Policja może udostępnić zasoby SPR-T jedynie Państwowej Straży Pożarnej, spełniającej te kryteria. Natomiast jednostki Ochotniczych Straży Pożarnych, nawet po włączeniu do KSRG, nie mogą korzystać z tego systemu, gdyż nie są jednostkami administracji publicznej.

Wdrożenie standardu DMR – wobec planów wprowadzenia jednolitego systemu łączności radiowej dla służb podległych MSWiA – może spowodować, że w przyszłości będą funkcjonować w PSP dwa niekompatybilne standardy (DMR oraz TETRA). W ramach pilotażu już wdrożono w KP PSP w Sokółce system oparty na DMR. Jednocześnie Z-ca Komendanta Głównego PSP zwrócił się do Z-cy Komendanta Głównego Policji z prośbą o wyrażenie zgody na rozpoczęcie i realizację procesu bezpłatnego testowania systemu radiokomunikacyjnego Policji TETRA (SRP-T) na terenie całego kraju od 12 czerwca 2024 r. W uzasadnieniu Komendant PSP wskazał, że skuteczna realizacja zadań wymaga niezawodnej i efektywnej komunikacji, a w ocenie Komendy Głównej PSP, oferowane funkcjonalności systemu SRP-T mogą znacząco usprawnić działania PSP, zwłaszcza w dużych aglomeracjach, poprzez szyfrowaną komunikację TEA2, wysoką niezawodność, szerokie możliwości integracji i interoperacyjności, zasięg i mobilność. Komendant wskazał również, że realizacja testów systemu TETRA, umożliwi ocenę jego funkcjonalności i przydatności w praktyce poprzez analizę skuteczności komunikacji

podczas akcji ratowniczych oraz zbadanie możliwości integracji z obecnie używanymi systemami radiokomunikacyjnymi.

W ocenie NIK ewentualne połączenie obu systemów w zakresie komunikacji głosowej za pomocą konsol integrujących może okazać się bardzo kosztowne w skali całego kraju i nie zapewni oczekiwanej od systemów cyfrowych funkcjonalności. Możliwe jednak, że w przyszłości udałoby się zintegrować oba systemy nie za pomocą obecnie dostępnych urządzeń, ale rozwijanej i testowanej obecnie na świecie technologii bram komunikacyjnych, takich jak Gateway IP i MCPTT IWF, umożliwiających translację protokołów między DMR, TETRA i LTE/5G. Dlatego istotne jest, by PSP realizowała budowę systemu z wykorzystaniem sieci IP, w tym infrastruktury OST112.

Standard DMR ma być wprowadzony w całej PSP do 2028 r., a standard TETRA jako podstawa dla SBŁP-T ma zostać wdrożony w całym kraju w perspektywie co najmniej sześciu lat. System DMR może się więc okazać przydatny jako system przejściowy w okresie budowania SBŁP-T, jednak Komendant Główny PSP powinien działać w ścisłym porozumieniu z Ministrem SWiA, tak aby ograniczyć ryzyko jednoczesnej budowy dwóch niezależnych systemów łączności dla PSP. Natomiast w wypadku podtrzymania decyzji o wdrożeniu DMR Komendant powinien szczegółowo zaplanować przeznaczenie systemu opartego na tym standardzie w sytuacji, gdy wprowadzony zostanie ogólnopolski system łączności radiowej dla służb w systemie TETRA.

Całkowite koszty wdrożenia nowego systemu w PSP nie zostały oszacowane do momentu zakończenia kontroli. PSP przyjęła model wdrożenia etapowego, oparty na pracy powoływanych lokalnie Zespołów ds. Wdrożenia Cyfrowej Łączności Radiowej, których zadaniem jest m.in. oszacowanie zakresu inwestycji wymaganych do migracji. Dzięki takiemu rozwiązaniu możliwa ma być migracja dokonywana kolejnymi krokami, z zachowaniem łączności z garnizonami, które jeszcze nie przeszły na system cyfrowy (co umożliwia standard DMR). NIK zauważa jednak konieczność priorytetowego potraktowania kwestii ustalenia kosztów wprowadzenia nowego systemu. Pozwoli to na sprawne podjęcie działań zmierzających do zapewnienia mechanizmów finansowania tego przedsięwzięcia.

5.2.3. STRAŻ GRANICZNA

**Straż Graniczna
wprowadziła spójny
system cyfrowej
łączności**

Straż Graniczna zdołała wprowadzić spójny system cyfrowej łączności radiowej w oparciu o standard DMR. Wdrożenie to zapoczątkował zaakceptowany w MSWiA w 2010 r. projekt pn. „Modernizacja systemów radiokomunikacyjnych Straży Granicznej”. W 2024 r. rozpoczęto

modernizację systemu łączności w SG¹⁷, która miała na celu m.in. zwiększenie mocy szyfrowania korespondencji radiowej.

System Służbowej Łączności Radiowej zbudowany został w całości z urządzeń pracujących w standardzie ETSI DMR, z szyfrowaniem oraz cyfrowym trybem pracy. Urządzenia te wyposażone były w funkcje m.in. wywołania grupowego, wywołania indywidualnego, szyfrowania bez utraty jakości i zasięgu, wysyłania SMS do grup oraz indywidualnych użytkowników, połączenia alarmowego, wysyłania alertów w chwili zagrożenia oraz zdalnego podsłuchu. Ponadto standard DMR umożliwiał pracę w trybie analogowym, co było przydatne np. w razie konieczności współpracy w ramach radiowej sieci współdzielenia służb MSWiA.

**W SG wykorzystywano
dodatkowe możliwości
cyfrowego sprzętu**

Straż Graniczna wykorzystywała dodatkowe możliwości cyfrowego systemu łączności. Jako system pomocniczy uruchomiono w tej służbie System Lokalizowania Radiotelefonów (SLR), który służył do lokalizowania patroli Straży Granicznej wyposażonych w radiotelefony pracujące w standardzie ETSI DMR. Ponadto SLR był źródłem przekazującym do Systemu Wspomagania Kierowania (SWK) pozycji GPS patroli polskiej Straży Granicznej oraz innych służb wykorzystujących infrastrukturę DMR SG. Mapa Sytuacyjna SWK przedstawiała lokalizację patroli Straży Granicznej wyposażonych w radiotelefony, a pozycje GPS radiotelefonów cyfrowych odzwierciedlały ich rzeczywistą lokalizację w terenie. Dodatkową funkcjonalnością mapy w SWK było zobrazowanie alarmów uruchomionych w radiotelefonach standardu ETSI DMR. Ponadto w Komendzie Głównej SG, Karpackim OSG i Nadbużańskim OSG wykorzystywany był dodatkowy system łączności DGT PTT Connect¹⁸, bazujący na bezprzewodowej transmisji danych i wykorzystujący również terminale działające w sieciach LTE/5G. System ten umożliwiał realizację połączeń grupowych, indywidualnych i priorytetowych oraz wysyłanie grupowych lub indywidualnych wiadomości tekstowych i multimedialnych.

Funkcjonariusze Straży Granicznej wykorzystywali system łączności DMR w trakcie realizacji zadań służbowych m.in. podczas: patroli, kontroli granicznej (osób, towarów i środków transportu) oraz w ramach służby dyżurnej operacyjnej. Łączność DMR w SG była również wykorzystywana do kontroli bezpieczeństwa, wykonywania czynności z zakresu działań minersko-pirotechnicznych i kontroli radiometrycznej. Ze środków

¹⁷ Modernizacją objęto Morski OSG, Podlaski OSG, Nadbużański OSG, Bieszczadzki OSG.

¹⁸ DGT PTT Connect to rozwiązanie typu Push-To-Talk, w którym zamiast klasycznych radiotelefonów wykorzystywane są terminale, pracujące z wykorzystaniem infrastruktury IP. DGT PTT Connect realizuje wszystkie funkcjonalności dostępne w cyfrowych systemach radiowych, a ponadto pozwala na szybkie przesyłanie zdjęć w wysokiej rozdzielczości lub innych plików np. planów, map, schematów, a wbudowany moduł mapowy pozwala śledzić pozycję wszystkich uczestników grupy.

łączności cyfrowej korzystano także przy doprowadzeniu osób oraz konwojowaniu broni, amunicji i dokumentacji służbowej. Ponadto, funkcjonariusze Straży Granicznej do celów komunikacji ze służbą dyżurną operacyjną i jednostkami współdziałającymi wykorzystywali alternatywnie – przy braku zasięgu łączności DMR – również łączność satelitarną, np. w trakcie służby na morzu na jednostkach pływających i na statkach powietrznych SG. Łączność satelitarna była wykorzystywana także do zabezpieczenia misji zagranicznych.

**System SG nie jest
kompatybilny
z planowanym
jednolitym systemem
łączności radiowej**

Przyjęty w SG standard łączności DMR nie jest kompatybilny ze standardem TETRA, w oparciu o który planowane jest utworzenie zintegrowanego systemu łączności radiowej dla służb podległych MSWiA. Potencjalna zmiana standardu łączności może spowodować, że w SG – podobnie jak w innych służbach – będą funkcjonowały równolegle dwa systemy łączności, oparte na dwóch niekompatybilnych standardach. Konsekwencjami takiego stanu rzeczy będą problemy z ich współpracą oraz zwiększone koszty utrzymania. NIK zwraca uwagę, że wprowadzenie w SG systemu DMR stanowiło z jednej strony odpowiedź na największe wady powszechnie stosowanej w naszym kraju łączności analogowej (w szczególności w zakresie bezpieczeństwa komunikacji), z drugiej strony jednak stworzyło ryzyko, że w przypadku wdrożenia systemu TETRA część dotychczas przyjętych rozwiązań może nie mieć uzasadnienia w potrzebach służby.

W kwestii wdrożenia w SG systemu cyfrowego opartego na standardzie DMR, a nie na standardzie TETRA wskazano, że ówczesne plany dotyczące wdrożenia systemu TETRA nie były wystarczająco precyzyjne, np. w zakresie terminów i obszarów, jakie miały być objęte pokryciem radiowym przedmiotowego systemu. Istotne natomiast było, aby zastąpić system analogowy cyfrowym systemem radiokomunikacyjnym, który umożliwiałby m.in. szyfrowanie korespondencji radiowej, prowadzonej pomiędzy patrolami SG. W związku z czym podjęto decyzję wdrożenia systemu pracującego w standardzie ETSI DMR, który oferował rozsądne możliwości w relacji do kosztu jego wdrożenia, m.in. uproszczoną migrację z systemu analogowego, ponieważ umożliwiał połączenie zarówno urządzeń analogowych, jak i cyfrowych. Kolejnym istotnym czynnikiem determinującym wybór standardu ETSI DMR było pasmo, w którym pracowały urządzenia ww. systemu oraz szerokość kanału radiowego, która pokrywała się z funkcjonującą wówczas w MSWiA siatką częstotliwości radiowych. Powyższe umożliwiała wykorzystanie dotychczas przydzielonych Straży Granicznej przez MSWiA kanałów radiowych.

5.2.4. SŁUŻBA OCHRONY PAŃSTWA

W ocenie SOP system łączności odpowiada potrzebom służby

System łączności radiowej w SOP opiera się na systemie NEXEDGE firmy Kenwood, który został wdrożony w 2010 roku i od tego czasu jest rozwijany. System ten zastąpił starsze rozwiązania wykorzystujące radiotelefony Motorola, które częściowo pozostały w użyciu. W ograniczonym zakresie wykorzystywany jest również system DMR firmy Keycera Mobile. Główny system składa się z łączności trunkingowej, wykorzystywanej do dowodzenia i koordynacji działań, łączności konwencjonalnej cyfrowej, stosowanej przez grupy ochronne oraz posterunki, a także łączności konwencjonalnej analogowej, używanej do współpracy z innymi instytucjami oraz w przypadkach braku kompatybilnych rozwiązań. Radiotelefony Kenwood i Motorola mogą komunikować się na kanałach analogowych, jednak bez funkcji maskowania transmisji. System łączności SOP spełnia kluczowe wymagania operacyjne, w tym możliwość zdalnego programowania i blokowania radiotelefonów, przesyłania krótkich wiadomości tekstowych oraz lokalizacji użytkowników za pomocą modułu GPS. Radiotelefony posiadają także funkcję wysyłania sygnału alarmowego do konsoli administratora. Kontrola wykazała, że około 75 proc. urządzeń Kenwood obsługiwało transmisję GPS. Pozytywnie zweryfikowana została funkcja zdalnego blokowania radiotelefonów.

W ocenie SOP wdrożony system łączności odpowiada potrzebom służby – charakteryzuje się wysoką niezawodnością i brakiem istotnych opóźnień w przekazywaniu komunikatów głosowych. Zapewnia maskowanie korespondencji, umożliwia elastyczne tworzenie grup korespondencyjnych oraz obsługuje kanały analogowe, co pozwala na współpracę z Policją i innymi służbami.

System SOP nie jest pozbawiony wad

Mimo że wdrożony system łączności SOP spełniał podstawowe wymagania operacyjne, to – w ocenie NIK – nie wszystkie jego funkcje i parametry odpowiadają standardom systemów dedykowanych dla służb bezpieczeństwa, co może wpływać na skuteczność realizowanych zadań, szczególnie w sytuacjach wymagających wysokiego poziomu zabezpieczenia i interoperacyjności (więcej o tym w kolejnym punkcie Informacji).

5.2.5. SZKOLENIE I WYPOSAŻENIE FUNKCJONARIUSZY

Funkcjonariuszom zapewniono szkolenie i sprzęt

Funkcjonariuszom każdej z kontrolowanych służb zapewniono szkolenie oraz wyposażenie niezbędne do obsługi systemów łączności radiowej. Komendanci poszczególnych służb uregulowali kwestie szkolenia w sposób formalny poprzez wydawanie odpowiednich rozkazów i decyzji, zapewniając tym samym spójność przygotowania funkcjonariuszy w obrębie danej formacji. W przypadkach niektórych jednostek

stwierdzono, że zasoby sprzętowe, wystarczające do realizacji codziennych zadań w ramach służby zmianowej, mogły okazać się niewystarczające w sytuacji kryzysowej, wymagającej pełnej mobilizacji wszystkich funkcjonariuszy. Braki te dotyczyły zarówno sprzętu cyfrowego w Policji oraz SG, co było wynikiem trwającego procesu wdrażania SRP-T oraz sytuacji na granicy polsko-białoruskiej. Także w SOP ilość sprzętu cyfrowego mogła pozostawać niewystarczająca, ponieważ funkcjonariuszom tej służby wciąż zdarzało się korzystać ze starszych analogowych radiotelefonów. Brakujący sprzęt pozostawał w planach zakupowych.

Badanie kwestionariuszowe przeprowadzone przez Izbę wykazało¹⁹, że funkcjonariusze służb podległych MSWiA na ogół doceniają wygodę korzystania z radiotelefonów oraz ich niezawodność. Jednocześnie wskazują na ich liczne ograniczenia techniczne. Najczęściej wymienianymi problemami były: 1. niewystarczający zasięg (83 proc. odpowiedzi), zła jakość połączenia (67 proc. odpowiedzi), brak możliwości przesyłania plików, takich jak zdjęcia, filmy, plany, schematy (49 proc. odpowiedzi). Dodatkowo funkcjonariusze zauważali w odpowiedziach brak możliwości nawiązania połączenia z innymi służbami za pomocą dedykowanego radiotelefonu (44 proc. odpowiedzi). Powszechnym oczekiwaniem respondentów (90 proc. odpowiedzi) było zastąpienie radiotelefonu urządzeniem hybrydowym, które umożliwiałoby nie tylko połączenie głosowe, ale realizowałoby funkcję wysyłania i odbierania danych.

Szkolenie policjantów z technologii i organizacji pracy w sieci łączności radiowej odbywało się podczas szkolenia zawodowego podstawowego, które obejmowało 12 godzin poświęconych tematowi „Posługiwanie się środkami łączności radiowej”. Po ukończeniu szkolenia podstawowego policjanci byli uprawnieni do pracy w sieci radiowej. Z kolei w ramach szkolenia oficerskiego, funkcjonariusze Policji byli zapoznawani z systemami łączności radiowej używanymi podczas akcji i operacji. Kurs specjalistyczny dla służby dyżurnej jednostek Policji obejmował sześć godzin lekcyjnych dotyczących obsługi systemów i urządzeń łączności na stanowisku kierowania. Dodatkowo, funkcjonariusze zdobywali wiedzę o systemach łączności radiowej podczas kursów specjalistycznych, takich jak kursy dla negocjatorów policyjnych i z zakresu poszukiwań osób zaginionych.

Funkcjonariusze Państwowej Straży Pożarnej kierowani byli na szkolenie podstawowe z zakresu łączności, które było realizowane zgodnie z „Programem szkolenia podstawowego w zawodzie strażak” i obejmowały dwie godziny teorii oraz dwie godziny praktyki w ramach

¹⁹ Wzięto w niej łącznie udział 119 funkcjonariuszy PSP i Policji. Więcej o wynikach ankiety na str. 65–66.

przedmiotu „Taktyka zwalczania pożarów”. Po ukończeniu szkolenia absolwenci otrzymywali zaświadczenie uprawniające do pracy w sieci radiowej ochrony przeciwpożarowej ważne przez 5 lat. Przedłużenie uprawnień wymagało odbycia szkolenia doskonalącego. W związku z planami wdrożenia cyfrowej łączności radiowej przed PSP stoi wyzwanie przeszkolenia kadry w zakresie niezbędnym do obsługi i nadzoru nad systemem DMR.

Obsługa systemu łączności VHF w Straży Granicznej wymagała ukończenia szkolenia podstawowego oraz okresowego. Szkolenia obejmowały przepisy i zasady prowadzenia korespondencji radiowej UKF oraz obsługę sprzętu łączności radiowej UKF. Szkolenia doskonalące użytkowników środków łączności były przeprowadzane co najmniej raz w roku i kończyły się testem zaliczeniowym. W związku z problemami na granicy polsko-białoruskiej oraz błędami użytkowników systemu łączności, zorganizowano szkolenia e-learningowe dla funkcjonariuszy i osób wspierających ochronę granicy.

Niedobory sprzętowe w Straży Granicznej

Kontrola wykazała niedobory sprzętowe w SG. W związku z sytuacją kryzysową związaną z masowym napływem cudzoziemców na polsko-białoruskim odcinku granicy państwowej, konieczne było wydanie przez SG ponad 1000 radiotelefonów nasobnych w celu zabezpieczenia w środki łączności radiowej posterunków obserwacyjnych, utworzonych wspólnie z Siłami Zbrojnymi RP. Odbyło się to m.in. poprzez przesunięcie znacznych ilości radiotelefonów z innych jednostek organizacyjnych SG, przez co w części z nich pojawiły się braki sprzętowe. Z kolei brak radiotelefonów przewoźnych spowodowany był wprowadzeniem do eksploatacji w SG znacznej liczby samochodów, które były sukcesywnie uzbrajane w sprzęt łączności. Niedobór stacji retransmisyjnych wynikał natomiast z braku wolnych środków na ich zakup, w związku z potrzebą rozbudowy SSŁR.

Przygotowanie funkcjonariuszy SOP do korzystania z systemów łączności odbywało się poprzez szkolenia zawodowe: podstawowe i uzupełniające, zgodnie z programami zatwierdzonymi przez Komendanta SOP. Uczestnicy szkoleń podstawowych musieli zaliczyć przedmiot „Łączność i informatyka” w formie testu i zadania praktycznego, natomiast uczestnicy szkoleń uzupełniających musieli uczestniczyć we wszystkich zajęciach.

W każdej ze służb pozostawały na wyposażeniu znaczące ilości radiotelefonów analogowych. Pełniły on różną rolę: w PSP i Policji były podstawowymi środkami łączności, w SOP uzupełniającymi, a w SG pomocniczymi – tj. używane były do łączności podczas prac naprawczych, serwisowych i instalacyjnych, podczas szkoleń oraz w celu zapewnienia łączności transgranicznej. Analogowy sprzęt łączności radiowej był też

traktowany przez służby jako potencjalny element łączności zapasowej do czasu zakończenia procesu jego wybrakowania.

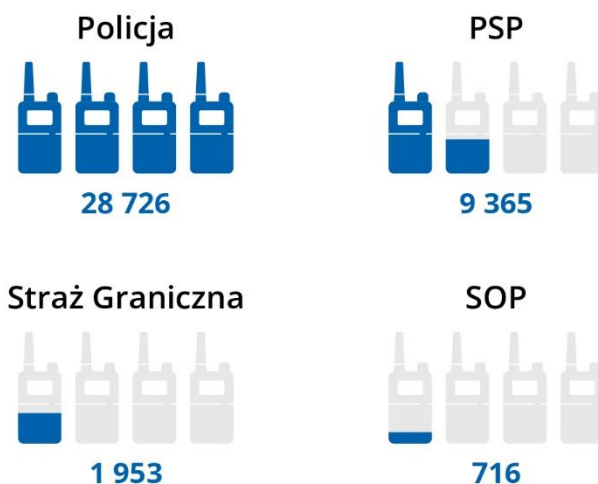
Analogowe radiotelefony były na tyle przestarzałe, że służby stanęły przed problemem braku możliwości ich uzupełnienia w przypadku awarii lub wybrakowania, ponieważ nie były one już oferowane przez producentów. W związku z tym służby, które nadal korzystały z systemów analogowych, zastępowały starsze radiotelefony urządzeniami pracującymi w technologii DMR, które mogły działać zarówno w trybie analogowym, jak i cyfrowym.

Należy uznać, że użytkowanie analogowych radiotelefonów w służbach porządku wewnętrznego stanowi zagrożenie dla bezpieczeństwa informacji oraz skuteczności operacyjnej (więcej o tym na s. 44), a proces ich wycofywania powinien zostać przyspieszony.

Infografika nr 3

Ilość sprzętu analogowego pozostającego na wyposażeniu służb (bez odniesienia do liczby funkcjonariuszy). Duża liczba radiotelefonów analogowych w Policji wynikała przede wszystkim z liczebności tej formacji.

Radiotelefony analogowe (różnego typu) pozostające na wyposażeniu służb:



Źródło: opracowanie własne NIK na podstawie danych przekazanych przez Policję, SG, PSP i SOP.

5.2.6. DŁUG TECHNOLOGICZNY W SYSTEMACH ŁĄCZNOŚCI SŁUŻB PODLEGŁYCH MSWiA

**Systemy łączności
służb pozostają w tyle
za rozwiązaniami
przyjętymi w Europie**

Kontrola wskazała na zjawisko długu technologicznego w obrębie systemów łączności radiowej wykorzystywanych przez służby podległe MSWiA, tj. odstawania infrastruktury i rozwiązań telekomunikacyjnych od aktualnych standardów i wymagań operacyjnych. Pojęcie to odnosi się do sytuacji, w której niedostateczne inwestycje w modernizację i spóźnione dostosowanie systemów skutkuje rosnącą liczbą problemów

technicznych, zwiększonym ryzykiem awarii oraz ograniczoną zdolnością do integracji z nowoczesnymi technologiami. W konsekwencji, choć formalnie funkcjonują, systemy te mogą nie zapewniać oczekiwanego poziomu niezawodności, bezpieczeństwa i wydajności, co w warunkach operacyjnych może prowadzić do zakłóceń w przekazywaniu informacji i utrudniać współpracę pomiędzy jednostkami. Pomimo podejmowanych przez poszczególnych komendantów działań modernizacyjnych oraz występowania nowoczesnych rozwiązań w wybranych przypadkach i na ograniczonym obszarze – systemy łączności radiowej wykorzystywane przez służby podległe MSWiA wykazują znamiona długu technologicznego.

**System SG ograniczony
dostępną pojemnością**

W najmniejszym stopniu zarzut ten dotyczy SG i SOP, tj. dwóch służb, które wdrożyły spójny system cyfrowej łączności radiowej. Pomimo tego kontrolerzy wskazali na słabości obu rozwiązań. W przypadku SG to przede wszystkim ograniczona pojemność systemu. Uwidoczniła się ona podczas intensyfikacji służby patrolowej na granicy polsko-białoruskiej. W tej sytuacji system łączności przyjęty w SG zbliżył się do granicy swojej pojemności (DMR zapewnia dwa kanały na jednej częstotliwości, podczas gdy TETRA oferuje cztery kanały komunikacyjne na jednej częstotliwości, w związku z czym pozwala obsługiwać więcej użytkowników jednocześnie, co jest istotne w dużych sieciach). Nie można wykluczyć, że intensywność użytkowania tego systemu będzie wzrastać, w związku z czym wskazane jest, aby SG wzięła to pod uwagę w swoich planach i koncepcjach dotyczących łączności radiowej. Należy także zauważyć, że w dobie rosnącego zapotrzebowania na przesyłanie danych, standard DMR jest ograniczony w tym zakresie i nie jest optymalny do takich zadań jak przesyłanie obrazów, map czy informacji telemetrycznych. Trzeba jednak zaznaczyć, że SG jako jedyna służba wdrożyła w całościowy sposób System Lokalizowania Radiotelefonów (SLR), który wykorzystywał radiotelefony pracujące w standardzie ETSI DMR, co opisano powyżej.

W przypadku SOP obciążająca dla systemu była kontynuacja eksploatacji systemu radiotelefonów analogowych, z których służba korzystała przed wprowadzeniem systemu NEXEDGE. Ich wykorzystanie do maskowanej korespondencji wiązało się z powstawaniem istotnych opóźnień podczas komunikacji, które – w przypadku ich użycia – mogły negatywnie wpływać na prowadzenie działań ochronnych. SOP zgodziła się z oceną NIK, że opóźnienia w korespondencji radiowej, wprowadzane przez pracujący moduł maskujący stosowany w Radiotelefonach Motorola, miały negatywny wpływ na jakość niektórych działań ochronnych.

Z kolei współpraca radiotelefonów cyfrowych i analogowych musiała być prowadzona otwartym tekstem bez maskowania. Korespondencja radiowa radiotelefonów Kenwood i Motorola zabezpieczona była za pomocą różnych funkcji maskowania, które nie były kompatybilne. W razie

**Niedostateczne
zabezpieczenie
komunikacji
w systemie SOP**

konieczności łączność pomiędzy radiotelefonami różnych systemów realizowana była w sposób otwarty.

Niewystarczająca była również sama technika maskowania. Maskowanie transmisji za pomocą *scramblingu* w NXDN zapewnia jedynie podstawowe zabezpieczenie przed przypadkowym podsłuchem, lecz jest łatwe do złamania metodą *brute force*. Brak silnego szyfrowania (takiego jak np. AES-128), naraża system na przechwytywanie transmisji przez osoby trzecie, co może stanowić zagrożenie bezpieczeństwa operacyjnego. Odbiorniki szerokopasmowe są zdolne do dekodowania sygnałów NXDN i są dostępne komercyjnie, co ułatwia potencjalny podsłuch. Odpowiednie narzędzia programowe umożliwiają z kolei analizę i inżynierię wsteczną protokołów radiowych, w tym NXDN, co zwiększa ryzyko przechwytywania danych.

Z punktu widzenia SOP ochrona danych w czasie rzeczywistym była zabezpieczeniem akceptowalnym, ponieważ przekazywane informacje w trakcie działań ochronnych miały znaczenie „tu i teraz”. Należy jednak zwrócić uwagę, że w ten sposób nie podlegała zabezpieczeniu tzw. technika operacyjna, której szczegóły, choć z opóźnieniem, mogła poznać osoba niepowołana. Dlatego istotne jest, by zrezygnować z używania *scramblingu* jako jedynego mechanizmu zabezpieczenia transmisji, ponieważ jest on niewystarczający w nowoczesnych systemach komunikacyjnych. Izba pozytywnie oceniła fakt, że jeszcze przed rozpoczęciem kontroli Komendant SOP podjął działania w celu usprawnienia systemu szyfrowania treści korespondencji radiowej, poprzez zakup licencji szyfrujących do radiotelefonów Kenwood oraz oprogramowanie do generowania kluczy szyfrujących.

**Dwie największe
służby posługują się
technologią
niepełniającą
standardów
operacyjnych**

W przypadku Policji i PSP podstawowym problemem pozostawało obciążenie przestarzałą technologią analogową. Jak wspomniano wyżej była ona podstawą łączności radiowej w 14 Komendach Wojewódzkich Policji (82,4 proc.) i w 201 Komendach Powiatowych (miejskich) Policji (58,6 proc.). W PSP łączność analogowa była podstawowym sposobem komunikacji radiowej. Pomimo zaangażowania funkcjonariuszy i pracowników Policji oraz PSP, odpowiedzialnych za łączność radiową, którzy maksymalizowali możliwości technologiczne systemów analogowych, dalsze utrzymywanie tych systemów w eksploatacji nie znajduje uzasadnienia. Radiowa technologia analogowa nie powinna być wykorzystywana przez służby porządku wewnętrznego i ratownictwa ze względu na jej ograniczone możliwości w zakresie bezpieczeństwa, jakości transmisji oraz efektywności operacyjnej. Brak zaawansowanego szyfrowania sprawia, że komunikacja jest podatna na przechwycenie, co stwarza ryzyko ujawnienia informacji operacyjnych. Jakość dźwięku w systemach analogowych jest niższa niż w cyfrowych, co utrudnia

zrozumienie komunikatów w trudnych warunkach akustycznych. Dodatkowo technologia ta nie wspiera nowoczesnych funkcji, takich jak zdalne zarządzanie urządzeniami, transmisja danych czy lokalizacja użytkowników, które znacząco podnoszą skuteczność działań. Ograniczona pojemność kanałów i podatność na zakłócenia mogą prowadzić do przeciążeń sieci i utrudnień w koordynacji operacji, co w sytuacjach kryzysowych stanowi istotne zagrożenie dla bezpieczeństwa publicznego i skuteczności służb.

**Pułapka
kompatybilności
wstecznej**

Należy również zwrócić uwagę, że wieloletnie opóźnienia w inwestycjach w nowoczesny system łączności radiowej oraz obciążenie wykorzystywaną przez służby łącznością analogową skutkowało zjawiskiem pułapki kompatybilności wstecznej. Pojęcie to oznacza sytuację, gdy konieczność zachowania zgodności z przestarzałym systemem prowadzi do wyboru rozwiązań suboptymalnych. Decyzja o wyborze standardu DMR zarówno przez SG, jak i PSP (na poziomie koncepcji) argumentowana była m.in. koniecznością zachowania kompatybilności z jednostkami, które w trakcie procesu wdrażania nowego systemu wciąż będą wykorzystywały technologię analogową (dodatkowo, jak wspomniano wyżej, w PSP nierozwiązanym problemem pozostaje kwestia OSP, w przypadku której wdrożenie systemu TETRA napotyka na barierę prawną). Obie służby uznały w tej sytuacji, że standard DMR – przy braku ogólnokrajowego rozwiązania opartego na standardzie TETRA – jest rozwiązaniem wystarczającym. Istotny był również argument, że urządzenia i infrastruktura DMR są tańsze oraz prostsze do wdrożenia. Chociaż więc to standard TETRA został zaprojektowany z myślą o profesjonalnych służbach odpowiedzialnych za bezpieczeństwo wewnętrzne i ratownictwo, oferując szereg funkcji spełniających wymagania operacyjne oraz ciągłość działania w krytycznych scenariuszach komunikacyjnych – SG i PSP zdecydowały się z opisanych wyżej powodów nie na rozwiązanie optymalne, ale w swojej ocenie wystarczające.

**Ryzyko długu
technologicznego**

Podtrzymanie długu technologicznego w służbach mundurowych może stanowić poważne zagrożenie dla ich efektywności operacyjnej oraz zdolności do szybkiego reagowania na współczesne wyzwania. W kontekście planowanego wprowadzenia systemu TETRA dopiero za sześć lat oraz jego ograniczonej przepustowości w zakresie transmisji danych, konieczne jest aktywne monitorowanie i wdrażanie nowoczesnych standardów telekomunikacyjnych, takich jak te opracowywane przez 3GPP dla usług Mission Critical (MCX).

Obecnie stosowane rozwiązania radiokomunikacyjne, choć zapewniają niezawodność w zakresie łączności głosowej, nie są dostosowane do rosnących wymagań dotyczących przesyłania dużych ilości danych, w tym obrazu i wideo. Funkcjonariusze coraz częściej wskazują na potrzebę

korzystania z urządzeń wielofunkcyjnych, które umożliwiałyby im przesyłanie zdjęć, nagrań i raportów w czasie rzeczywistym. Obecna infrastruktura nie spełnia tych oczekiwań, co zmusza służby do korzystania zarówno z przestarzałych radiotelefonów, jak i prywatnych smartfonów, tworząc nieefektywną i potencjalnie niebezpieczną sytuację operacyjną.

Inne państwa
wdrażają łączność
szerokopasmową

Przykład

Francja realizuje zaawansowany projekt modernizacji komunikacji krytycznej – *Réseau Radio du Futur* (RRF), który ma zastąpić przestarzałe systemy łączności radiowej używane przez służby. Projekt ogłoszony w 2017 roku otrzymał 700 mln euro na lata 2023–2027 i jest wdrażany przez Ministerstwo Spraw Wewnętrznych. RRF to sieć 4G/5G zapewniająca priorytet, mechanizm *preemption*²⁰ i interoperacyjność dla służb bezpieczeństwa oraz zarządzania kryzysowego. Wdrażany w modelu *Hybrid Government – Commercial Networks*, łączy infrastrukturę operatorów komercyjnych z rządową kontrolą nad krytycznymi funkcjami sieci. W 2023 roku osiągnięto kluczowe etapy:

zbudowano architekturę RRF i rozpoczęto wdrażanie usług, uruchomiono infrastrukturę w data center i chmurze Ministerstwa, rozpoczęto testy end-to-end oraz integrację w kilku centrach danych. Do 2027 roku RRF ma objąć 300 tys. użytkowników, zapewniając 98 proc. pokrycia terytorium i pełne wsparcie komunikacyjne dla służb ratowniczych. Dodatkowo wdrożono aplikację SYRIUS – do grupowej komunikacji, geolokalizacji i transmisji danych – oraz SRR, rozwiązanie wzmacniające zasięg w sytuacjach kryzysowych.

Rekomendacje dla
podmiotów
odpowiedzialnych za
wdrożenie systemu
cyfrowej łączności

Wyniki kontroli wskazują, że zasadnym jest śledzenie i adaptowanie rozwiązań telekomunikacyjnych opartych na LTE i 5G, które oferują znacznie większą przepustowość i możliwości integracji z istniejącymi systemami. Standardy 3GPP dla usług MCX umożliwiają stopniowe i płynne przejście służb mundurowych na nowoczesną infrastrukturę, jednocześnie zapewniając kompatybilność z tradycyjnymi systemami radiowymi. Pominięcie tego aspektu w planowaniu przyszłych rozwiązań komunikacyjnych państwa grozi dalszym zwiększaniem długu technologicznego, co w konsekwencji może prowadzić do obniżenia poziomu bezpieczeństwa publicznego i efektywności działania służb. Dlatego kluczowe jest, aby już na etapie projektowania nowej

²⁰ Mechanizm zarządzania priorytetami transmisji, który pozwala na przerywanie lub ograniczanie połączeń o niższym priorytecie, aby zrobić miejsce dla transmisji krytycznych lub o wyższym priorytecie. Jest kluczowy dla służb ratunkowych, wojska i administracji państwowej, zapewniając im niezawodną łączność nawet w warunkach przeciążenia sieci.

infrastruktury komunikacyjnej uwzględnić technologie szerokopasmowe oraz standardy MCX. Ich implementacja pozwoli na stworzenie spójnego i wydajnego systemu, który nie tylko sprosta obecnym wymaganiom, ale również umożliwi elastyczne dostosowanie się do przyszłych wyzwań technologicznych i operacyjnych.

**Konieczność
uwzględnienia
nowoczesnych
standardów dla usług
krytycznych**

Rekomendacje eksperta NIK

1. Należy śledzić inicjatywę pn. Europejski System Komunikacji Krytycznej (EUCCS), która promuje interoperacyjność krytycznej komunikacji w oparciu o technologie MCX (MCPTT, MCVideo, MCDATA) zgodne ze standardami 3GPP. Kluczowe projekty, takie jak BroadMap i BroadWay, wspierają harmonizację technologii na poziomie UE.
2. Należy przyglądać się standardom 3GPP dla usług Mission Critical (MCX), które przewidują szerokie możliwości integracji systemów radiokomunikacji lądowej (LMR), takich jak DMR i TETRA, z sieciami LTE/5G poprzez zastosowanie funkcji Interworking Function (IWF). Uwzględnienie tych standardów w projektowaniu docelowej sieci komunikacyjnej dla Państwa jest kluczowe, aby zapewnić pełną interoperacyjność między tradycyjnymi systemami radiowymi a nowoczesnymi rozwiązaniami opartymi na technologiach LTE i 5G.
3. Należy przeprowadzić szczegółową analizę istniejących wdrożeń technologii MCX w służbach ratowniczych i porządku publicznego na świecie w celu zidentyfikowania najlepszych praktyk, oceny możliwości interoperacyjności oraz określenia wyzwań związanych z adaptacją tych rozwiązań do polskich realiów operacyjnych.
4. Zaleca się wykorzystanie Gateway IP jako zaawansowanego rozwiązania do translacji protokołów i integracji TETRA oraz DMR poprzez infrastrukturę IP, co usprawni komunikację między lokalizacjami. Rekomenduje się także zastosowanie MCPTT IWF, zgodnego ze standardami 3GPP, aby osiągnąć najwyższy poziom integracji, umożliwiając współpracę technologii LTE/5G z LMR przy pełnej kontroli nadawania i obsłudze zaawansowanych funkcji krytycznych, takich jak Mission Critical Push-To-Talk.
5. Rekomenduje się wdrożenie Interworking Function (IWF) w celu zapewnienia płynnej interoperacyjności między technologiami LTE/5G a systemami tradycyjnymi (TETRA, DMR). IWF umożliwi transkodowanie, zarządzanie kluczami szyfrowania oraz wysoką dostępność systemu, co czyni go odpowiednim rozwiązaniem dla zastosowań wymagających niezawodności w sytuacjach krytycznych.

5.2.7. WYKORZYSTYWANIE TELEFONII KOMÓRKOWEJ PRZEZ SŁUŻBY

**Telefonia komórkowa
odpowiedzią na
niewydolność
dedykowanych
systemów**

Miarą niewystarczalności dedykowanych systemów łączności w służbach było wykorzystywanie przez nie cywilnej telefonii komórkowej. Służby nie regulowały tego zagadnienia lub wprost pozwalały swoim funkcjonariuszom na korzystanie z telefonów komórkowych, w tym prywatnych, szczególnie w sytuacji braku możliwości połączenia za pomocą radiotelefonu.

I tak w PSP funkcjonariusze posiadali dostęp do służbowych telefonów komórkowych, które były wykorzystywane jako dodatkowy środek komunikacji, zwłaszcza w sytuacjach, gdy tradycyjne systemy radiowe były niewystarczające lub w przypadku potrzeby szybkiej komunikacji indywidualnej. W sytuacjach awaryjnych dopuszczono w PSP możliwość wykorzystania prywatnych telefonów komórkowych.

W SOP poza zasięgiem radiotelefonów noszonych i przewoźnych oraz w obszarach nieobjętych stałą lub mobilną infrastrukturą przekaźnikową, służbowe telefony komórkowe stanowiły podstawowy środek łączności ruchomej. Nie określono zasad wykorzystania prywatnych telefonów komórkowych do celów służbowych.

W SG funkcjonariusze do wykonywania zadań służbowych używali również telefonów komórkowych, co do zasady służbowych. Na dziewięć oddziałów SG telefony komórkowe były wykorzystywane do czynności służbowych w sześciu, a w dwóch dopuszczono możliwość korzystania z prywatnych telefonów komórkowych w przypadkach niesprawności systemu łączności radiowej.

W Policji nie opracowano uregulowań dotyczących wykorzystania prywatnych telefonów komórkowych do celów służbowych. W codziennych działaniach funkcjonariusze mogą korzystać z telefonów komórkowych i są one powszechnie wykorzystywane w sytuacjach niewymagających natychmiastowego reagowania. Jednocześnie w toku kontroli ustalono, że wybór środka łączności zależy nie tylko od specyfiki działania, ale także od dostępności infrastruktury.

Przykład

- W KPP w Grójcu funkcjonariusze wykorzystywali w służbie prywatne telefony komórkowe w sytuacjach, gdy ukształtowanie terenu lub specyfika danego miejsca uniemożliwiały nawiązanie łączności za pomocą etatowego systemu radiowego. W takich wypadkach dopuszczano możliwość kontaktu z dyżurnym Komendy Powiatowej Policji poprzez połączenie z numerem stacjonarnym, wyposażonym w rejestrator rozmów. Rozwiązanie to pozwalało na przekazanie niezbędnych informacji, takich jak

potwierdzenie przybycia na miejsce zdarzenia czy zakończenie jego obsługi.

- W związku z tym, że dedykowane systemy łączności nie umożliwiały przesyłania danych, w KP PSP w Ostródzie podczas prowadzonych działań wykorzystywano telefony komórkowe. Za ich pośrednictwem przekazywano głównie zdjęcia, a sporadycznie także materiały wideo z miejsca zdarzenia lub akcji ratowniczej. Pliki te przesyłano na służbowy telefon komórkowy przypisany do Stanowiska Kierowania Komendanta Powiatowego. Ponadto Komendant dopuszczał możliwość przesyłania w ten sam sposób funkcjonariuszom przez dyżurnego Stanowiska Kierowania informacji istotnych dla przebiegu akcji ratowniczej, takich jak karty charakterystyki substancji niebezpiecznych czy fragmenty instrukcji bezpieczeństwa pożarowego obiektu.
- Komendant Śląskiego Oddziału Straży Granicznej, w nawiązaniu do problemu niewystarczającego zasięgu dedykowanego systemu łączności DMR w trudnych warunkach terenowych, wyjaśnił, że w razie potrzeby funkcjonariusze działający w terenie wyposażeni są w służbowe telefony komórkowe, które mogą zostać wykorzystane jako alternatywny środek łączności.

NIK nie neguje zasadności wykorzystywania telefonów komórkowych w działalności operacyjnej służb. Urządzenia te znajdują szerokie i uzasadnione zastosowanie, np. w przypadku funkcjonariuszy pełniących służbę w charakterze dzielnicowych, którym umożliwiają bieżący kontakt z mieszkańcami oraz szybkie uzyskiwanie informacji. Nie mogą one jednak stanowić substytutu dla dedykowanego systemu łączności radiowej. Zastępowanie profesjonalnych rozwiązań telekomunikacyjnych telefonami komórkowymi, wynikające z niewydolności systemu radiowego, prowadzić może do ograniczenia skuteczności działań operacyjnych oraz zwiększa ryzyko zakłóceń w sytuacjach kryzysowych.

**Zagrożenia związane
z niewłaściwym
wykorzystywaniem
telefonów
komórkowych**

Należy również zwrócić uwagę na zagrożenia wynikające z wykorzystywania przez służby cywilnej telefonii komórkowej w sytuacji potencjalnego konfliktu zbrojnego i konieczności uruchomienia obrony cywilnej. Może ona zostać zakłócona lub całkowicie wyłączona przez wrogie siły, co skutkowałoby utratą zdolności do koordynacji działań ratowniczych. Ponadto telefony komórkowe mogą być wykorzystywane do śledzenia lokalizacji użytkowników, co stwarza ryzyko namierzenia i zaatakowania funkcjonariuszy oraz ratowników przez przeciwnika. Precyzyjne uderzenia wymierzone w kluczowe elementy służb odpowiedzialnych za utrzymanie porządku i niesienie pomocy mogą prowadzić do szerzenia terroru wśród ludności cywilnej oraz obniżenia skuteczności państwa.

Ustalenia kontroli dotyczące wykorzystania telefonów komórkowych przez funkcjonariuszy znalazły potwierdzenie w ankiecie przeprowadzonej przez NIK. Blisko 97 proc. funkcjonariuszy przyznało, że w ciągu ostatnich dwóch lat skorzystało z telefonu komórkowego zamiast radiotelefonu. Głównymi przyczynami były: brak możliwości połączenia za pomocą dedykowanego systemu radiowego, dostępność dodatkowych funkcji nieobecnych w radiotelefonie (np. nawigacja z uwzględnieniem bieżącej sytuacji na drodze), lepsza jakość komunikacji głosowej oraz możliwość nawiązania kontaktu z funkcjonariuszami innej służby. Potrzebę zastąpienia radiotelefonu urządzeniem będącym odpowiednikiem smartfona, które umożliwiłoby zarówno łączność radiową, jak i przesyłanie danych (zdjęcia, plany itp.), wyraziło 90 proc. ankietowanych funkcjonariuszy.

5.2.8. PROBLEMY KADROWE W ZAKRESIE OBSŁUGI SYSTEMÓW TELEINFORMATYCZNYCH

W trakcie kontroli stwierdzono, że w każdej z badanych służb występuje problem związany z niedostateczną liczbą administratorów lub specjalistów odpowiedzialnych za obsługę systemów radiowej łączności cyfrowej. Zidentyfikowano także trudności w pozyskiwaniu wykwalifikowanego personelu, co stanowi istotne wyzwanie w kontekście planowanego rozwoju tych systemów.

Państwowa Straż Pożarna zmagą się z istotnym niedoborem specjalistów z zakresu teleinformatyki oraz administratorów łączności, co może wpływać na skuteczność wdrażania i funkcjonowania zaplanowanego systemu cyfrowej łączności radiowej. Zgodnie z Raportem kadrowym w obszarze IT zatwierdzonym przez Komendanta Głównego PSP w październiku 2024 r., standardy branżowe określają zalecane proporcje personelu IT do liczby użytkowników na poziomie:

- 1:82 według standardu Robert Half Technology (2008),
- 1:70 do 1:200 według standardu Gartnera (w zależności od wielkości organizacji),
- 1:18 do 1:27 według Workforce.

Przykład

W PSP współczynnik zatrudnienia osób z wykształceniem teleinformatycznym do całkowitej liczby użytkowników systemu wynosił 1:728 – stanowi to znaczące odstępstwo od wskazanych wyżej norm i może skutkować problemami w bieżącej eksploatacji oraz implementacji nowych technologii.

**PSP mierzy się
z kryzysem kadrowym
pod względem
zatrudnienia
teleinformatyków**

W PSP przyjęto, że optymalnym poziomem zatrudnienia dla koordynatorów ds. cyfrowej łączności radiowej w procesie wdrażania systemu DMR będzie jeden specjalista na 100–150 użytkowników systemu. Jednym z kluczowych czynników utrudniających osiągnięcie tego poziomu może być brak dodatku teleinformatycznego dla tej służby. Wynika to z faktu, że PSP nie została uwzględniona w wykazie podmiotów uprawnionych do świadczenia teleinformatycznego na podstawie art. 5 ustawy z dnia 2 grudnia 2021 r. o szczególnych zasadach wynagradzania osób realizujących zadania z zakresu cyberbezpieczeństwa²¹. Mimo podejmowanych od czerwca 2022 r. przez Komendanta Głównego PSP działań mających na celu objęcie PSP tymi regulacjami, Państwowa Straż Pożarna pozostaje jedyną służbą mundurową podległą MSWiA, która nie otrzymuje środków z Funduszu Cyberbezpieczeństwa, co znacząco ogranicza możliwość konkurencyjności o specjalistów na rynku pracy. Minister SWiA poinformował, że podczas prac nad zmianą ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw²². Ministerstwo zgłosiło uwagi dotyczące włączenia PSP do katalogu podmiotów, których pracownicy byłiby uprawnieni do otrzymywania świadczenia teleinformatycznego (projekt w trakcie rządowego procesu legislacyjnego, na początku lutego 2025 roku nadal znajdował się w procesie legislacyjnym, a jego ostateczne przyjęcie i wejście w życie są planowane na najbliższe miesiące; obecnie dostępne informacje na temat projektu nie wskazują na wprowadzenie poprawek przyznających funkcjonariuszom i pracownikom PSP prawa do otrzymywania świadczenia teleinformatycznego).

Dodatkowym problemem wskazanym w ww. Raporcie był brak jednoznacznego przypisania zarządzania sieciami radiokomunikacyjnymi do kompetencji pracowników IT w regulaminach organizacyjnych PSP. Może to prowadzić do opóźnień w konserwacji systemów oraz wzrostu ryzyka operacyjnego. W celu poprawy sytuacji, PSP planuje wdrożenie kompleksowych programów szkoleniowych obejmujących obsługę systemów radiowych, zarządzanie interoperacyjnością oraz zapewnienie niezawodności komunikacji w sytuacjach kryzysowych. Działania te mają na celu poprawę efektywności zarządzania infrastrukturą teleinformatyczną i łączności w PSP oraz minimalizację ryzyk związanych z niedoborem wyspecjalizowanej kadry.

**Zwiększone
zapotrzebowanie na
specjalistów w Policji**

Z analizy przeprowadzonej przez Policję wynikało, że braki kadrowe w obszarze cyfrowej łączności radiowej były spowodowane m.in. niskim wynagrodzeniem w stosunku do ofert rynkowych przy jednoczesnym oczekiwaniu od kandydatów bardzo wysokich kwalifikacji. W samej KGP

²¹ Dz. U. z 2024 r. poz. 1662.

²² Projekt nr UC32 <https://legislacja.rcl.gov.pl/projekt/12384504>.

potrzeby kadrowe w zakresie wykwalifikowanych specjalistów do sprawnego zarządzania cyfrową łącznością radiową (w tym administratorów) wynosiły na 30 września 2024 r. 36 etatów, przy czym zatrudnionych było 10 osób – tj. niespełna 28 proc. Potrzeby Policji zwiększały się w związku z operacyjnym wdrożeniem SRP-T (TETRA TEA2), rozbudową tego systemu i koniecznością dalszego planowania i zwiększenia zakresu usług, liczby i rodzajów użytkowników. Komendant Główny Policji określił problem kadrowy służby w tym obszarze – tj. niedostępność osób z odpowiednimi kwalifikacjami oraz w praktyce brak możliwości systemowego pozyskiwania specjalistów z zakresu teleinformatyki – jako duży i zidentyfikował go jako jeden z głównych problemów w rozbudowie i integracji systemu SRP-T.

**Niewystarczająca
liczba specjalistów
łączności w SG**

Także w SG niewystarczająca pozostawała liczba osób zajmujących się utrzymaniem sprawności systemu, zarówno w części oddziałów, jak i w samej KG SG. W 2022 r. w Wydziale Telekomunikacji KGSG za administrowanie systemem łączności odpowiedzialnych było pięć osób. W związku z odejściami ze służby w kolejnych latach zadania te realizowały już tylko trzy osoby. W ocenie Dyrektora Biura była to liczba niewystarczająca do prawidłowej realizacji zadań związanych z administrowaniem SSŁR.

**SOP zminimalizowała
wymagania
kwalifikacyjne**

Problemy kadrowe w obszarze specjalistów od łączności nie ominęły SOP. Odpowiednia komórka zajmująca się radiokomunikacją obejmowała 28 etatów. Na dzień 21 listopada 2024 r. zatrudnionych było w niej dziewięciu funkcjonariuszy (w tym ośmiu zajmujących się radiokomunikacją) oraz dwóch pracowników cywilnych. Stan ukończenia wynosił więc około 40 proc., co uniemożliwiało realizację zadań w standardowym czasie pracy i wymuszało pracę ponadnormatywną (nadgodziny). Aby uzupełnić braki kadrowe stosowano wobec kandydatów minimalne wymagania kwalifikacyjne: poszukiwano techników z wykształceniem średnim technicznym, pracowników ze znajomością obsługi komputera i programów takich jak MS Office oraz zdolnością do szybkiego przyswajania wiedzy technicznej. Służba Ochrony Państwa starała się pozyskać nowych pracowników poprzez promocję na targach pracy i w mediach społecznościowych. Dodatkowo prowadzone były działania rekrutacyjne wśród kursantów SOP, funkcjonariuszy innych służb oraz byłych funkcjonariuszy i żołnierzy posiadających specjalistyczną wiedzę techniczną w zakresie łączności radiowej. Proces rekrutacji przynosił jednak ograniczone rezultaty – w 2024 r. zatrudniono jednego funkcjonariusza. Dyrektor odpowiedniej komórki wskazał, że specjalistów ds. łączności radiowej jest niewielu, a wynagrodzenia w tym sektorze są mniej konkurencyjne niż w IT.

Funkcjonariusze i pracownicy Policji, SG oraz SOP mogli otrzymywać świadczenie teleinformatyczne z Funduszu Cyberbezpieczeństwa, zgodnie z zasadami określonymi w rozporządzeniu Rady Ministrów z dnia 19 stycznia 2022 r. *w sprawie wysokości świadczenia teleinformatycznego dla osób realizujących zadania z zakresu cyberbezpieczeństwa*²³. Było ono czynnikiem podtrzymującym zatrudnienie w służbie specjalistów z zakresu teleinformatyki i łączności. Wysokość wypłacanego świadczenia uwarunkowano doświadczeniem zawodowym, posiadaną wiedzą oraz zakresem zadań realizowanych w obszarze cyberbezpieczeństwa. NIK stwierdziła, że w poszczególnych służbach podległych Ministrowi SWiA zasady przyznawania dodatku dla osób realizujących zadania z zakresu bezpieczeństwa teleinformatycznego, tzw. świadczenia teleinformatycznego, nie były wystarczająco wystandaryzowane względem siebie i wynikały z wewnętrznych decyzji kierownictwa Policji, SOP i Straży Granicznej. Kryteria – takie jak doświadczenie zawodowe czy posiadanie specjalistycznej wiedzy – wpływały jedynie na maksymalną kwotę świadczenia, nie precyzując jednak konkretnych zasad ustalania jego wysokości w ramach określonego przedziału. Taka konstrukcja przepisów pozostawia szeroki margines interpretacyjny dla osób odpowiedzialnych za przyznawanie świadczenia teleinformatycznego. W praktyce oznacza to, że wysokość świadczenia może być w znacznej mierze uzależniona od indywidualnej oceny przyznającego. Ponadto funkcjonariusze i pracownicy PSP – jak wspomniano wyżej – w ogóle nie zostali wskazani w ustawie o szczególnych zasadach wynagradzania osób realizujących zadania z zakresu cyberbezpieczeństwa, co postawiło tę służbę w bardzo trudnej sytuacji wobec planowanego przez nią wdrożenia łączności cyfrowej DMR.

5.2.9. NIEDOSTATECZNE PRZYGOTOWANIE SYSTEMÓW ŁĄCZNOŚCI NA SYTUACJE KRYZYSOWE

Powyższe problemy – wykorzystywanie przestarzałych lub suboptymalnych technologii, zastępowanie dedykowanych systemów radiowych cywilną telefonią komórkową, brak odpowiedniej liczby teleinformatyków specjalizujących się w cyfrowej łączności – składają się na niewystarczające przygotowanie służb podległych MSWiA do sytuacji kryzysowych. Istnieje ryzyko, że w przypadku uszkodzenia infrastruktury telekomunikacyjnej lub zorganizowanego ataku cybernetycznego, funkcjonariusze mogą utracić czasowo możliwość skutecznego porozumiewania się, co osłabi zdolność do reagowania na zagrożenia i koordynacji działań operacyjnych.

²³ Dz. U. z 2022 r. poz. 131.

**Doświadczenia służb
pozyskane w trakcie
działań związanych
z powodzią na Dolnym
Śląsku**

Przypuszczenia te potwierdziła sytuacja kryzysowa spowodowana powodzią na Dolnym Śląsku w 2024 r. Zalanie oraz brak zasilania spowodowały wyłączenie części stacji bazowych w Kotlinie Kłodzkiej, co doprowadziło do przerw w działaniu sieci telefonii komórkowej. Operatorzy tacy jak Orange, Play i Plus informowali o tych trudnościach i podejmowali działania mające na celu przywrócenie pełnej funkcjonalności sieci. W szczytowym momencie około 71 tysięcy odbiorców pozostawało bez zasilania z powodu uszkodzeń na stacjach transformatorowych. Problemy z łącznością i komunikacją znacząco utrudniały działania ratunkowe oraz koordynację pomocy dla poszkodowanych. Także służby zidentyfikowały w tej sytuacji szereg problemów związanych z infrastrukturą radiokomunikacyjną i organizacją łączności. Kluczowym wyzwaniem był brak łączności na potrzeby zarządzania kryzysowego pomiędzy poszczególnymi służbami i podmiotami zaangażowanymi w proces pomocy poszkodowanym. W celu przezwyciężenia tych problemów PSP zastosowała m.in. połączenie sieciowe pięciu radioprzemienników DMR przy wykorzystaniu infrastruktury IP, pozwalając na stworzenie jednolitego systemu komunikacyjnego obejmującego duży obszar (co było organizowaną na bieżąco namiastką oczekiwanego w Polsce nowoczesnego systemu radiowego odpornego na sytuacje kryzysowe). Wykorzystano także terminale satelitarne Starlink. Ponieważ PSP nie posiadała wystarczającej ich liczby, konieczna okazała się pomoc innych podmiotów. Służby wsparł m.in. Instytut Łączności – PIB. W rezultacie 160 takich zestawów zostało rozmieszczonych w kluczowych punktach działań ratowniczych i potrzeb dla ludności cywilnej, zapewniając łączność w miejscach, gdzie tradycyjna infrastruktura telekomunikacyjna została uszkodzona.

MSWiA w koncepcji utworzenia SBŁP-T (opartego na standardzie TETRA) zakłada, że będzie on również pełnił funkcję systemu na czas kryzysu, pod warunkiem jego odpowiedniej rozbudowy. System TETRA został zaprojektowany do działania w trudnych warunkach, np. podczas katastrof czy ataków terrorystycznych. Nie jest zależny od komercyjnych sieci GSM – w przypadku awarii sieci komórkowych służby nadal będą mogły się porozumiewać. Funkcja Direct Mode (DMO) – pozwala na komunikację między radiotelefonami (choć o ograniczonym zasięgu) nawet bez dostępu do infrastruktury sieciowej, np. w razie awarii stacji bazowych. Dla zachowania odporności na sytuacje kryzysowe stacje bazowe wymagają własnego źródła zasilania – eksperci z Instytutu Łączności zwrócili uwagę, że należy o tym pamiętać przy planowaniu infrastruktury systemu. Zapewnienie takiego źródła może być jednak problematyczne przy długotrwałych kryzysach.

**SG planuje system
zapasowej łączności**

Na podstawie doświadczeń ostatnich kilku lat SG doszła do wniosku, że podstawowe środki łączności sprawdzają się do wymiany informacji

w warunkach pokoju i braku poważniejszych zagrożeń, natomiast w sytuacjach kryzysowych oraz czasie zagrożenia konfliktem zbrojnym są narażone na uszkodzenia systemów zasilania oraz systemów sieciowej infrastruktury przewodowej i bezprzewodowej, co czyni je systemami zawodnymi w takich warunkach. Z tego powodu w 2024 r. Komendant Główny Straży Granicznej zaakceptował koncepcję budowy zapasowego systemu łączności radiowej. Ma być on oparty na podstawowej łączności satelitarnej zapewniającej łączność głosową dowództwu, systemie opartym na satelitach LEO (np. Starlink) lub MEO²⁴ (pod warunkiem spełnienia przez nie wymagań SG) oraz krótkofalowej łączności radiowej KF.

Problemy z łącznością satelitarną na stanowiskach kierowania Policji

Kontrola wykazała niedostatecznie przygotowanie jednostek dowódczych Policji i SOP do sytuacji kryzysowych. W KGP łączność awaryjną na wypadek kryzysu stanowił telefon satelitarny na stanowisku kierowania (dowodzenia) oraz dwa radiotelefony w systemie TETRA. W wyniku przeprowadzonych oględzin ustalono, że Policja nie była w stanie nawiązać łączności za pomocą telefonu satelitarnego z żadną ze wskazanych przez kontrolerów jednostek. I Zastępca Komendanta Głównego Policji wyjaśnił, że wpływ miały na to warunki pogodowe oraz zabudowa terenu. NIK zwróciła jednak uwagę, że łączność satelitarna jest przeznaczona do wykorzystania w trudnych warunkach, a wspomniana zabudowa terenu pozostaje względnie niezmienna. Brak możliwości połączenia satelitarnego tworzył więc ryzyko dla właściwej koordynacji dowodzenia, szczególnie w sytuacji kryzysowej (według deklaracji KGP łączność w takich sytuacjach zapewniały także funkcjonujące sprawnie radiotelefony TETRA, przy pomocy których udało się nawiązać łączność).

Policja używała systemu INMARSAT, posiadającego węzły komunikacyjne na terenie Federacji Rosyjskiej

Kontrola wskazała także na występujący w Policji do grudnia 2023 r. problem polegający na wykorzystywaniu systemu łączności satelitarnej INMARSAT. Stan techniczny użytkowanych zestawów łączności satelitarnej INMARSAT uniemożliwiał ich dalszą eksploatację ze względu na znaczne zużycie i awaryjność sprzętu oraz braki podzespołów serwisowych na rynku. Stwierdzono także, że systemy te posiadają tzw. węzły komunikacyjne na terenie Federacji Rosyjskiej, co stwarzało dodatkowe zagrożenia dla użytkowników końcowych. System ten zastąpiono

²⁴ Systemy LEO i MEO (Low i Medium Earth Orbit) – konstelacja satelitów działająca na niskiej orbicie okołoziemskiej (LEO). Przykładowo Satelity Starlink krążą na wysokości od około 340 km do 570 km nad Ziemią, co pozwala na zmniejszenie opóźnień w komunikacji i zwiększenie przepustowości w porównaniu do tradycyjnych systemów satelitarnych na orbicie geostacjonarnej (GEO – 35 786 km). Z kolei systemy działające na średniej orbicie okołoziemskiej (MEO), jak O3b mPOWER, operują na wysokości od 2 000 km do 35 786 km i często są wykorzystywane w zastosowaniach wojskowych i telekomunikacyjnych.

**Centralne Stanowisko
Kierowania SOP bez
połączenia
satelitarnego i TETRA**

systemem IRIDIUM, który zapewnić ma bezpieczeństwo prowadzonej korespondencji i dodatkowo pełną interoperacyjność z Siłami Zbrojnymi RP.

W Centralnym Stanowisku Kierowania SOP łączność zapasową stanowiły telefony satelitarne oraz radiotelefon TETRA, jednak podczas przeprowadzonych oględzin nie udało się nawiązać połączenia przy ich użyciu. Dyrektor Zarządu XII wskazał na możliwość występowania licznych czynników zakłócających działanie telefonii satelitarnej, zobowiązując się do ich identyfikacji i eliminacji. Kontrolerzy ustalili jednak, że system telefonii satelitarnej w CSK SOP osiągnął status „końca cyklu życia” (EOL) w czerwcu 2023 r., co oznacza brak wsparcia technicznego oraz aktualizacji. Dokumentacja techniczna wskazuje, że wpływ warunków atmosferycznych na jakość sygnału była ograniczona, a głównymi przyczynami zakłóceń mogły być uszkodzenia lokalnej infrastruktury lub nieprawidłowe ustawienie anteny. Z kolei brak łączności przez radiotelefon TETRA wynikał ze zmiany zasad szyfrowania przez Komendę Stołeczną Policji, która udostępniła sprzęt SOP. Aktualizacja oprogramowania w CSK SOP nastąpiła dopiero dzień po kontroli, mimo że zmiana systemu szyfrowania miała miejsce cztery miesiące wcześniej. Stwierdzone niesprawności sprzętowe mogły negatywnie wpłynąć na koordynację działań, reakcję na zagrożenia oraz podejmowanie decyzji w czasie rzeczywistym, zwłaszcza w sytuacjach kryzysowych wymagających współdziałania z Policją.

**Brak skutecznej
interoperacyjności
w sytuacjach
kryzysowych**

Ważnym elementem gotowości systemu łączności radiowej służb na sytuacje kryzysowe jest jego zdolność do zapewnienia skutecznej współpracy między różnymi formacjami odpowiedzialnymi za bezpieczeństwo oraz działania ratownicze. W warunkach kryzysowych, takich jak katastrofy naturalne, zagrożenia terrorystyczne czy inne sytuacje nadzwyczajne – interoperacyjność systemów łączności, czyli możliwość ich efektywnego współdziałania, stanowi kluczowy czynnik determinujący skuteczność reakcji służb w sytuacjach wymagających ich wspólnego zaangażowania. Kontrola wykazała jednak, że obecny system łączności radiowej służb nie zapewnia skutecznej współpracy między formacjami w sytuacjach kryzysowych, co może prowadzić do utrudnień w koordynacji działań i opóźnień w reakcji na zagrożenia.

5.2.10. PRZEGLĄDY TECHNICZNE MASZTÓW I INSTALACJI ANTENOWYCH

Kontrola wykazała liczne nieprawidłowości w zakresie przeprowadzania okresowych przeglądów technicznych masztów i instalacji antenowych, które stanowią ważny element infrastruktury łączności radiowej wykorzystywanej przez służby podległe MSWiA. Zgodnie z art. 62 ust. 1

**Liczne
nieprawidłowości
dotyczące przeglądów
instalacji antenowych**

ustawy Prawo budowlane²⁵, obiekty budowlane, w tym maszty i wieże antenowe, powinny być poddawane okresowym przeglądom co najmniej raz w roku w celu sprawdzenia ich stanu technicznego oraz wykrycia potencjalnych uszkodzeń mogących zagrażać ich stabilności i bezpieczeństwu użytkowania.

W dziewięciu jednostkach na czternaście – właściwych do wykonania takich przeglądów – stwierdzono nieprawidłowości o różnej skali i zakresie, w tym: brak przeprowadzania wymaganych przeglądów rocznych, zaniedbania w prowadzeniu dokumentacji technicznej, opóźnienia w realizacji kontroli i nieusuwanie wykrytych usterek. Dotyczyły one czterech jednostek Policji, czterech jednostek Państwowej Straży Pożarnej oraz jednego Oddziału Straży Granicznej. Problemy te wynikały przede wszystkim z niewłaściwego nadzoru nad infrastrukturą, braku środków finansowych na realizację przeglądów oraz konserwację masztów i instalacji antenowych, a także nieprzekazywania informacji o koniecznych działaniach naprawczych.

Przykład

- W Komendzie Wojewódzkiej Policji w Olsztynie w latach 2022–2023 nie przeprowadzano corocznych przeglądów dla wszystkich 27 skontrolowanych masztów.
- W Komendzie Powiatowej Państwowej Straży Pożarnej w Ostródzie brak kontroli dotyczył 80 proc. instalacji antenowych.
- W Komendzie Wojewódzkiej Policji w Szczecinie w ogóle nie realizowano corocznych przeglądów w latach 2022–2023.
- W Komendzie Wojewódzkiej Policji w Rzeszowie spośród 95 masztów aż 93 (97,9 proc.) wymagało pilnych działań naprawczych.
- W Komendzie Wojewódzkiej Policji zs. w Radomiu w 2022 r. przeglądów nie przeprowadzono dla 98 proc. masztów.
- W jednej z sześciu placówek Śląskiego Oddziału Straży Granicznej przez trzy kolejne lata nie realizowano zaleceń konserwacyjnych, mimo wcześniejszych kontroli wskazujących na konieczność podjęcia działań naprawczych.
- W Komendzie Powiatowej PSP w Raciborzu wieża antenowa od 2016 r. nie została poddana żadnej kontroli technicznej, co oznacza, że przez osiem lat funkcjonowała bez jakiegokolwiek oceny jej stanu.
- W Komendzie Miejskiej PSP w Świnoujściu przez dwa lata (2022–2023) nie przeprowadzono przeglądu technicznego masztu antenowego zamontowanego na dachu budynku Komendy.

²⁵ Dz.U. z 2024 r. poz. 725.

Stwierdzone nieprawidłowości w zakresie przeglądów masztów i instalacji antenowych świadczą o braku skutecznego nadzoru oraz niewystarczającym zabezpieczeniu środków finansowych na ten cel. W wielu jednostkach przeglądy były realizowane nieregularnie, a w skrajnych przypadkach całkowicie zaniechane, co istotnie zwiększa ryzyko wystąpienia awarii infrastruktury łączności radiowej i mogło stwarzać zagrożenie dla zdrowia i życia ludzkiego.

5.3. INTEROPERACYJNOŚĆ SYSTEMÓW ŁĄCZNOŚCI RADIOWEJ

Brak jednolitego systemu łączności radiowej istotną przeszkodą w komunikacji służb

Brak jednolitego systemu łączności radiowej stanowił istotną barierę dla interoperacyjności systemów służb podległych MSWiA, utrudniając ich współdziałanie, zwłaszcza w sytuacjach kryzysowych. Obecne rozwiązania, takie jak kanał B112, nie spełniają wymogów bezpieczeństwa i niezawodności, przez co służby rzadko z niego korzystają. Pozytywnym przykładem efektywnej współpracy była grupa radiowa RATUNEK, której funkcjonowanie pokazało potencjalne korzyści z ogólnokrajowego jednolitego systemu łączności. Jej uruchomienie było możliwe dzięki wdrożeniu przez Policję systemu TETRA w czterech miastach: Warszawie, Krakowie, Łodzi i Szczecinie. Jednocześnie wobec ograniczeń funkcjonowania tego systemu wyłącznie do czterech miast poszczególne formacje próbowały sobie radzić w różny sposób – od delegowania oficerów łącznikowych po wykorzystywanie telefonii komórkowej, co nie gwarantowało skutecznej komunikacji operacyjnej. Ustalenia kontroli pokazują, że nowoczesny, jednolity system łączności cyfrowej sprzyja pozostawianiu służb w stałej komunikacji ze sobą, usprawnia koordynację działań i zwiększa ich efektywność, podczas gdy stosowanie przestarzałych, niekompatybilnych rozwiązań technologicznych prowadzi do funkcjonowania służb w rozproszonym modelu, w którym łączność utrzymywana jest w sytuacjach wymuszonych okolicznościami często jedynie poprzez kontakt fizyczny.

5.3.1. KANAŁ B112

Słabości kanału B112 jako narzędzia współdziałania służb

Kanał B112, jako radiowa sieć współdziałania służb MSWiA, został stworzony z założeniem zapewnienia łączności między formacjami odpowiedzialnymi za bezpieczeństwo publiczne i ratownictwo. Jego celem była możliwość bezpośredniej wymiany informacji w miejscu prowadzenia działań, szczególnie w sytuacjach kryzysowych, wymagających skoordynowanej reakcji. Pomimo opracowania zasad jej użytkowania sieci i jej formalnego funkcjonowania, wyniki kontroli wykazały, że w praktyce służby resortu MSWiA nie korzystały z niej podczas realizowanych działań. Sporadyczne przypadki jej użycia ograniczały się głównie do ćwiczeń

i testów (choć i w tych sytuacjach pomijano kanał B112), co wskazuje na niską efektywność tego rozwiązania.

Przykład

- Z informacji przekazanych kontrolerom przez warszawską Policję wynikało, że żadna z jednostek i komórek organizacyjnych Komendy nie była w stanie ustalić kiedy wykorzystano kanał B112 po raz ostatni w akcji.
- Jednym z wniosków po ćwiczeniach przeprowadzonych przez Policję z innymi służbami MSWiA, wojskiem i instytucjami realizującymi zadania porządku i bezpieczeństwa publicznego było niedostateczne wykorzystanie kanału B112 – większość korespondencji przekazywana była przy wykorzystaniu telefonów komórkowych, a nie dedykowanej sieci współpracy.

Podstawową słabością kanału B112 był jego analogowy charakter, który nie odpowiada współczesnym standardom łączności stosowanym w służbach bezpieczeństwa publicznego. Sieć działa w trybie simplex, co oznacza, że transmisja odbywa się jednokierunkowo, bez możliwości jednoczesnego nadawania i odbierania komunikatów. Ograniczony zasięg, podatność na zakłócenia i brak zabezpieczeń przed dostępem osób nieuprawnionych stanowią istotne zagrożenie dla skuteczności i bezpieczeństwa komunikacji. Brak szyfrowania transmisji powoduje ryzyko podsłuchiwania, a w skrajnych przypadkach – zakłócania komunikacji przez podmioty zewnętrzne.

Zidentyfikowano również problemy organizacyjne związane z użytkowaniem kanału. Kontrola wykazała, że na stanowiskach kierowania i dowodzenia nie prowadzono bieżącego nasłuchu B112 – zgodnie z przyjętymi zasadami – a jego doraźne uruchomienie wymagało wcześniejszego uzgodnienia telefonicznego. W praktyce oznaczało to, że sieć nie była dostępna natychmiast w sytuacji wymagającej szybkiej i skoordynowanej reakcji. Ponadto MSWiA nie gromadziło danych na temat korzystania z sieci przez poszczególne służby, co utrudniało ocenę jej rzeczywistej przydatności operacyjnej.

Minister wskazał, że jednolity standard analogowy przyjęto w celu zapewnienia kompatybilności sprzętu używanego przez różne formacje, w tym Policję, PSP, Straż Graniczną i SOP, a także inne podmioty odpowiedzialne za bezpieczeństwo. Z uwagi na zróżnicowanie stosowanych w służbach systemów radiowych, w tym sieci konwencjonalnych, DMR i NEXEDGE, jedyną możliwością zapewnienia wspólnej komunikacji było wykorzystanie kanału VHF z modulacją F3E. Jednak przyjęcie tego rozwiązania kosztem nowoczesnych technologii ograniczyło możliwości operacyjne i skuteczność współpracy.

**Służby wykorzystują
kanał B112
sporadycznie**

Minister stwierdził też, że służby resortu MSWiA nie zgłaszały potrzeby modyfikacji zasad pracy w sieci B112. W opinii NIK dowodzi to jedynie tego, że ograniczona funkcjonalność sieci była powszechnie akceptowana lub pomijana w codziennym działaniu. Jednocześnie wykazano, że na miejscu akcji służby często wykorzystywały inne metody współpracy, w tym udostępnianie własnego sprzętu łączności, co podkreśla niedostosowanie kanału B112 do realnych potrzeb operacyjnych.

Ustalenia kontroli znalazły potwierdzenie w ankiecie przeprowadzonej przez NIK. Blisko 86 proc. ankietowanych funkcjonariuszy przyznało, że w ciągu ostatnich dwóch lat nie używało kanału B112 w celu współpracy z funkcjonariuszami innych służb. Kolejne 9,3 proc. używało tego kanału jedynie w trakcie ćwiczeń. Tylko 5 proc. funkcjonariuszy zadeklarowało użycie w okresie objętym kontrolą kanału B112 zgodnie z przeznaczeniem. Jednocześnie 52 proc. ankietowanych przyznało, że do połączenia z funkcjonariuszami innej służby użyło telefonu komórkowego.

5.3.2. WYKORZYSTANIE SYSTEMU TETRA PRZEZ SŁUŻBY

**System trunkingowy
umożliwił skuteczną
komunikację między
służbami**

Faktyczną interoperacyjność służb można było uzyskać w miastach, w których działał cyfrowy system łączności radiowej oparty na standardzie TETRA. System taki został uruchomiony przez Policję w czterech aglomeracjach: Warszawie, Krakowie, Łodzi i Szczecinie. Integrację policyjnego systemu łączności z innymi służbami osiągnięto poprzez zawieranie dwustronnych porozumień, które włączały inne służby lub podmioty do systemu TETRA administrowanego przez Policję lub rozszerzały zasięg tego systemu dzięki użyczonej infrastrukturze. Przykładowo Komendant Stołeczny Policji zawarł takie porozumienia m.in. z Urzędem m. st. Warszawy, Mazowieckim Komendantem Wojewódzkim Państwowej Straży Pożarnej oraz z Metrem Warszawskim Sp. z o.o. Podstawowym celem porozumień było wdrożenie jednolitego systemu łączności radiowej na potrzeby grupowej łączności na obszarze terytorialnym stolicy. System taki podnosił poziom ciągłości działania oraz umożliwiał tworzenie grup współpracy (z PSP, Strażą Miejską, Zarządem Dróg Miejskich).

Modelowym przykładem wykorzystania jednolitego systemu cyfrowej łączności jest działanie w stolicy grupy radiowej RATUNEK (w oparciu o policyjną sieć TETRA). Stałymi jej abonentami były następujące stanowiska zgłoszeń: Dyżurny Komendy Stołecznej Policji, Dyżurny Operacyjny Komendy Miejskiej Państwowej Straży Pożarnej w Warszawie, Dyspozytor Wojewódzkiej Stacji Pogotowia Ratunkowego, Służba Dyżurna Stołecznego Centrum Bezpieczeństwa m. st. Warszawy, Dyżurny Wojewódzkiego Centrum Zarządzania Kryzysowego, Dyżurny Centralnego Stanowiska Kierowania Straży Miejskiej m. st. Warszawy. Sieć

**Wady modelu
opartego na
porozumieniach**

funkcjonowała w trybie ciągłego nasłuchu, co zapewniało bieżącą interoperacyjność służb.

Należy mieć jednak na uwadze, że sieć działała przede wszystkim z zachowaniem potrzeb i interesów Policji, niezbędnych dla realizowanych przez nią zadań. Ograniczenie takiego rozwiązania uwidoczniło się przy konieczności modernizacji sieci (przejście do systemu SRP-T o wyższym standardzie szyfrowania). W związku z nią stwierdzono ograniczenia w funkcjonowaniu grupy RATUNEK. Przykładowo część stanowisk PSP, która do tej pory miała dostęp do sieci, utraciła ją z powodu niedostosowania urządzeń do nowej wersji systemu TETRA. W SOP radiotelefony służące do pracy w tej sieci pozostały niezaktualizowane przez kolejne cztery miesiące i przez ten czas nie miały dostępu do systemu. Mimo tych ograniczeń funkcjonowanie grupy RATUNEK jest dowodem na to, że zintegrowany system cyfrowej łączności radiowej znacząco usprawnia współdziałanie służb i podnosi poziom bezpieczeństwa. Przykład ten pokazuje, jak mogłyby funkcjonować formacje ratownicze i porządkowe na terenie całego kraju, gdyby wdrożono jednolity ogólnopolski system łączności. Pełne rozwinięcie takiego rozwiązania pozwoliłoby na eliminację dotychczasowych barier w komunikacji między służbami i znacząco zwiększyłoby skuteczność działań w sytuacjach wymagających natychmiastowej reakcji i ścisłej koordynacji.

5.3.3. WSPÓŁPRACA SŁUŻB W WARUNKACH BRAKU JEDNOLITEGO SYSTEMU ŁĄCZNOŚCI

**Liczne porozumienia
pomiędzy służbami**

Współpraca służb podległych MSWiA oraz innych formacji odpowiedzialnych za bezpieczeństwo i ratownictwo była formalnie regulowana licznymi porozumieniami określającymi zasady współdziałania w zakresie łączności radiowej. Zawierane umowy dotyczyły zarówno bieżącej koordynacji działań, jak i organizacji współpracy podczas wydarzeń wymagających wspólnych operacji. Wśród najważniejszych dokumentów znalazło się porozumienie pomiędzy Komendantem Głównym Policji, Komendantem Głównym Straży Granicznej, Komendantem Głównym PSP oraz Biurem Ochrony Rządu, które określało ramy współdziałania i zakładało dążenie do wypracowania jednolitych rozwiązań w zakresie systemów łączności. Porozumienia zawierano także na poziomie wojewódzkim i lokalnym. Przykładowo Komenda Wojewódzka Policji w Rzeszowie uregulowała współpracę ze Strażą Graniczną w zakresie wykorzystania środków łączności na podstawie dwóch porozumień. Porozumienie z 9 maja 2008 r. określało zasady organizowania i utrzymywania łączności podczas wspólnych działań poprzez wzajemne udostępnianie sieci radiowych i systemów łączności. Natomiast porozumienie z 2 października 2015 r. regulowało wzajemne udostępnianie zasobów logistycznych, w tym infrastruktury radiowej

i telekomunikacyjnej, w celu zapewnienia łączności radiowej i przewodowej dla realizacji zadań pionów łączności i informatyki.

Pomimo licznych porozumień, współpraca w zakresie łączności radiowej miała w dużej mierze charakter formalny i nie przekładała się na realne usprawnienie komunikacji operacyjnej. Wobec braku jednolitego systemu łączności, porozumienia te koncentrowały się na doraźnym dostosowywaniu dostępnych środków, jednak w praktyce nie usuwały barier technologicznych ani nie zapewniały pełnej interoperacyjności.

Przykład

Przykładem interesującego porozumienia, a jednocześnie problemów służb ze wspólną łącznością radiową, jest współpraca pomiędzy Stołeczną Policją a Służbą Ochrony Państwa. W 2021 roku w Komendzie Stołecznej Policji odnotowano obszarową blokadę łączności, spowodowaną działaniem urządzenia zagłuszającego (tzw. *jammer*) wykorzystywanego przez SOP do zabezpieczeń VIP. Urządzenie to, mające na celu uniemożliwienie zdalnej detonacji ładunków wybuchowych, zakłócało również komunikację radiową Policji. W odpowiedzi na ten problem przedstawiciele KSP i SOP przeprowadzili robocze spotkanie, podczas którego uzgodniono parametry pracy urządzeń, tak aby umożliwić działanie policyjnej sieci.

Łączność w warunkach kryzysu na granicy z Białorusią

Weryfikacją możliwości wspólnej komunikacji między służbami był kryzys na granicy polsko-białoruskiej, podczas którego zaistniała konieczność współpracy operacyjnej SG, Policji oraz Sił Zbrojnych RP. W sytuacji niekompatybilności systemów łączności, posiadanych przez te formacje, podjęto próbę ich integracji na poziomie sprzętowym. W grudniu 2021 r. w Placówce SG w Lipsku uruchomiono integrator łączący system TETRA użytkowany przez żołnierzy Sił Zbrojnych RP z systemem DMR Straży Granicznej, a następnie na bazie tego samego urządzenia przeprowadzono integrację w rejonie odpowiedzialności służbowej Placówki SG w Nowym Dworze. W ramach kolejnych działań zapewniających zestawienie łączności w połowie stycznia 2022 r. uruchomiono kolejny integrator w terytorialnym zasięgu działania placówek SG w Szudziałowie oraz w Krynkach. W wyniku przeprowadzonych działań uzyskano możliwość połączenia głosowego między służbami. Jednocześnie stwierdzono, że objęło ono swoim obszarem jedynie część odcinków odpowiedzialności służbowej poszczególnych placówek Straży Granicznej. Powodem miały być ograniczenia wynikające z zasięgów stacji bazowych systemu TETRA, co uniemożliwiło dalszą integrację.

Wobec braku możliwości sprzętowej integracji systemów łączności służby były zmuszone do stosowania prowizorycznych rozwiązań, takich jak

wymiana radiotelefonów między formacjami. Przykładem jest przekazywanie wojsku radiotelefonów Straży Granicznej czy wzajemna wymiana urządzeń pomiędzy Policją a SG, które po zakończeniu działań były zwracane. Wymagało to dodatkowej alokacji sprzętu, co obciążało zasoby jednostek i komplikowało logistykę operacyjną. Ponadto takie rozwiązanie obciążało system łączności SG, który zbliżył się do granic swoich możliwości.

Kontrola wykazała także, że w sytuacjach wymagających współdziałania różnych formacji, niedoskonałości systemu łączności radiowej zmuszały funkcjonariuszy do posilkowania się telefonią komórkową jako głównym środkiem komunikacji operacyjnej. Przykładem jest sytuacja związana z działaniami funkcjonariuszy Nadodrzańskiego Oddziału Straży Granicznej, którzy wspierali Policję podczas demonstracji przed komendą NoOSG w lutym 2022 r., uczestniczyli w ćwiczeniach PSP w Krośnie Odrzańskim oraz brali udział w działaniach przeciwpowodziowych we wrześniu 2024 r. W wymienionych przypadkach wystąpiły problemy z nawiązaniem łączności radiowej, co znacząco utrudniało koordynację działań. Główną przyczyną miała okazać się niewystarczająca liczba radioprzemienników, które przy niekorzystnie ukształtowanym terenie nie zapewniały pełnego pokrycia sygnałem na całym obszarze działania służb. Wobec tych ograniczeń funkcjonariusze zmuszeni byli do korzystania z telefonów komórkowych w celu utrzymania łączności między patrolami.

**Interoperacyjność
w praktyce codziennej
służby**

Ustalenia kontroli wykazały, że w sytuacji braku jednolitego systemu łączności radiowej funkcjonariusze różnych służb stosują w codziennej praktyce alternatywne sposoby komunikacji w celu zapewnienia koordynacji działań. Najczęściej wykorzystywane metody obejmują: połączenia telefoniczne, zarówno komórkowe, jak i stacjonarne; oddelegowanie oficerów łącznikowych, pełniących rolę pośredników w przekazywaniu informacji między służbami; kontakt bezpośredni, polegający na wymianie informacji podczas osobistych spotkań funkcjonariuszy na miejscu działań.

Przykład

Zgodnie z wyjaśnieniami Komendanta Powiatowego w Grójcu, dotyczącymi sposobu komunikacji z innymi służbami, policjanci tej komendy przy akcjach poszukiwawczych i wypadkach drogowych najczęściej współpracują z funkcjonariuszami Państwowej Straży Pożarnej lub jednostkami Ochotniczych Straży Pożarnych ujętymi w KSRG. Funkcjonariusze obu służb przy realizacji ww. zadań pozostają w bezpośrednim kontakcie osobistym. Powyższy sposób komunikacji zapewnia zdaniem komendanta skuteczność działań.

**Ograniczenia
systemowe utrudniają
koordynację działań**

Ustalenia kontroli wskazują jednak, że poleganie na komunikacji bezpośredniej jako głównej metodzie wymiany informacji pomiędzy służbami stanowi rozwiązanie niewystarczające, zwłaszcza w sytuacjach wymagających szybkiej koordynacji i działania na rozległym obszarze. Kontakt osobisty, choć istotny w niektórych aspektach współpracy, nie może zastąpić sprawnie funkcjonującego systemu łączności radiowej, który umożliwia natychmiastowe przekazywanie informacji do wszystkich zaangażowanych jednostek jednocześnie.

Co więcej, brak jednolitego systemu łączności radiowej może prowadzić do utrudnień w koordynacji działań, szczególnie w przypadku akcji wymagających współdziałania większej liczby służb w różnych lokalizacjach. W takich przypadkach konieczność fizycznego przekazywania informacji pomiędzy funkcjonariuszami może powodować opóźnienia i ograniczać zdolność do dynamicznego reagowania na zmieniające się warunki operacyjne. Również łączność telefoniczna i wymiana oficerów łącznikowych obciążone są słabościami, m.in. zależnością od infrastruktury cywilnej, która może okazać się zawodna w sytuacji kryzysowej. Z kolei przekazywanie informacji za pośrednictwem oficerów łącznikowych może prowadzić do opóźnień, błędnej interpretacji przekazu lub utraty kluczowych danych. Taki sposób przekazywania informacji bywa nazywany w środowisku specjalistów od łączności radiowej „zabawą w głuchy telefon”.

Stosowane w praktyce metody komunikacji wynikają z ograniczeń systemowych, a nie z optymalnego modelu współpracy. Choć pozwalają na doraźne zapewnienie komunikacji operacyjnej, ich skuteczność jest ograniczona w porównaniu do jednolitego systemu łączności radiowej. Utrzymanie skuteczności działań operacyjnych wymaga wdrożenia nowoczesnych rozwiązań telekomunikacyjnych, które zapewnią służbom niezawodną, bezpieczną i natychmiastową wymianę informacji, minimalizując ryzyka wynikające z obecnych ograniczeń.

5.4. NADZÓR MINISTRA SWiA

Nadzór Ministra nad podległymi mu służbami²⁶ – w zakresie funkcjonujących w nich systemów łączności radiowej – nie był dostateczny. W kontroli stwierdzono, że Minister nie posiadał pełnej wiedzy i nie gromadził na bieżąco danych dotyczących budowy i rozwoju użytkowanych w Policji, Straży Granicznej, Państwowej Straży Pożarnej i Służbie Ochrony Państwa sieci i systemów radiokomunikacyjnych, w szczególności danych o wielkości nakładów poniesionych na ich

²⁶ Pełniony na podstawie Ustawy o nadzorze.

**Niedostateczna
wiedza Ministra
o funkcjonowaniu
systemów łączności**

funkcjonowanie, potrzebach związanych z rozbudową oraz problemach operacyjnych.

Na potrzeby kontroli Minister był w stanie udostępnić jedynie dane o wydatkach z Programu modernizacji zrealizowanych w okresie od początku 2022 r. do połowy 2024 r. w ramach przedsięwzięcia „Sprzęt informatyki i łączności”, tj. łącznych wydatków dotyczących systemów telekomunikacyjnych i radiokomunikacyjnych (szacunkowo ok. 103 mln zł). Nie potrafił przy tym określić, jaka suma została przeznaczona wyłącznie na systemy radiowe. Dopiero Pełnomocnik Ministra do spraw organizacji SBŁP przekazał kontrolującym kwoty łącznych kosztów poniesionych przez poszczególne służby w latach 2016–2023, które zebrał w III kwartale 2024 r.

NIK zauważyła też, że Minister nie miał wiedzy o przyjętej przez PSP w grudniu 2023 r. koncepcji migracji do cyfrowego systemu łączności w standardzie DMR, pomimo że przedstawiciele DT MSWiA współpracowali ze Strażą Pożarną na różnych etapach przygotowania tego planu. Do końca kontroli Minister nie pozyskał przedmiotowego dokumentu, a jedynie informację Komendanta, że ma on charakter wewnętrzny i zawiera wstępne założenia do planowanej zmiany łączności radiowej w PSP. Sytuacja ta, w ocenie NIK, świadczy o braku bieżącej współpracy i nadzoru nad działaniami służby w tym obszarze oraz może prowadzić do poniesienia przez PSP niezasadnych wydatków – szczególnie wobec realizowanych w MSWiA prac na rzecz wdrożenia jednolitego systemu łączności cyfrowej TETRA, z którym DMR nie jest kompatybilny.

NIK stwierdziła też, że Minister nie dysponował wiedzą o niewielkiej przydatności radiowej sieci współdziałania służb MSWiA, którą wskazał jako narzędzie do nawiązania łączności w sytuacji bezpośredniej współpracy. Przyjęte zasady organizacji radiowej sieci współdziałania określały możliwość komunikacji między funkcjonariuszami różnych służb z użyciem łączności analogowej VHF na niezabezpieczonym kanale radiowym B112. W kontroli wykazano, że – jak wspomniano wyżej – służby resortu SWiA nie wykorzystywały sieci współdziałania i kanału radiowego B112 do realizacji zadań wymagających wspólnych działań. Sporadycznie testowano kanał podczas prowadzonych ćwiczeń, stwierdzając m.in. trudności związane z brakiem zabezpieczeń i przestarzałą techniką komunikacji.

Przykład

Znaczącym przykładem braku nadzoru Ministra nad funkcjonowaniem łączności w służbach MSWiA podczas działań w sytuacji kryzysowej był fakt, że nie posiadał on informacji o działaniach podjętych przez poszczególne służby dla zapewnienia łączności między funkcjonariuszami podczas powodzi w południowo-zachodnim

regionie Polski i stanu klęski żywiołowej w II połowie 2024 r. Tym samym MSWiA nie wiedziało, jakie trudności wystąpiły w komunikacji służbowej oraz jakich urządzeń i systemów użyto, by zapewnić łączność w sytuacji kryzysowej.

Przytoczone ograniczenia wynikały przede wszystkim z niedostatecznego nadzoru Ministra nad komórkami organizacyjnymi MSWiA, wyznaczonymi do realizacji ww. zadania. Ustalono, że Departament Teleinformatyki MSWiA, który miał prowadzić m.in. sprawy w zakresie planowania i rozwoju łączności radiowej w podległych służbach i innych organach, realizował powyższe zadania w bardzo ograniczonym zakresie. W toku kontroli uzyskano wyjaśnienia Ministra, że działanie departamentu polegało na przyznawaniu służbom zasobów częstotliwości radiowych, według zgłaszanych przez nich potrzeb, oraz że nie realizowano innych działań związanych z funkcjonowaniem systemów łączności radiowej w podległych mu służbach. Minister poinformował też, że DT prowadził jedynie nadzór nad budową oraz wdrożeniem infrastruktury ogólnokrajowego cyfrowego systemu łączności radiowej dla potrzeb Ministra i służb resortu SWiA i nie prowadził nadzoru zadań związanych w ogólności z organizacją i funkcjonowaniem systemów łączności radiowej w podległych służbach. Przy tym inne departamenty MSWiA nadzorujące w imieniu Ministra podległe służby²⁷ nie realizowały zadań związanych z nadzorem nad funkcjonowaniem w nich systemów łączności.

**Brak specjalistów
w komórkach
organizacyjnych
MSWiA**

NIK zauważyła, że na realizację zadań w DT MSWiA negatywnie mógł wpływać brak wykwalifikowanych pracowników, specjalistów w zakresie radiokomunikacji. We właściwym wydziale, wyznaczonym do realizacji wskazanych zadań dotyczących radiowych systemów łączności, w okresie objętym kontrolą odnotowano istotne zmniejszenie stanu kadrowego. Do połowy 2023 r. w Wydziale Radiokomunikacji i Systemów Satelitarnych zatrudnionych było dwóch pracowników, następnie jeden, a od lutego 2024 r. w DT MSWiA nie było żadnego pracownika etatowo realizującego zadania z zakresu radiokomunikacji.

W ocenie NIK nierzetelny sposób sprawowania nadzoru przez Ministra nad organizacją i funkcjonowaniem łączności radiowej w podległych mu służbach mógł przyczynić się do opóźnienia we wdrażaniu jednolitego ogólnokrajowego systemu radiowej łączności cyfrowej dla służb resortu SWiA oraz innych podmiotów działających w strukturze zarządzania kryzysowego.

²⁷ Departament Porządku Publicznego sprawujący nadzór nad Policją, Strażą Graniczną i Służbą Ochrony Państwa i Departament Ochrony Ludności i Zarządzania Kryzysowego (nadzór nad Państwową Strażą Pożarną).

6. ZAŁĄCZNIKI

6.1. METODYKA KONTROLI I INFORMACJE DODATKOWE

Cel główny kontroli	Głównym celem kontroli było sprawdzenie czy system łączności radiowej w służbach podległych Ministrowi Spraw Wewnętrznych i Administracji funkcjonuje właściwie.
Cele szczegółowe	Przyjęto, że badania kontrolne umożliwią udzielenie odpowiedzi na następujące pytania szczegółowe: 1. Czy przyjęte koncepcje i zasady funkcjonowania łączności radiowej w służbach podległych Ministrowi Spraw Wewnętrznych i Administracji odpowiadały ustalonym standardom w obszarze bezpieczeństwa, porządku publicznego i ratownictwa oraz były ze sobą spójne? 2. Czy wykorzystywane przez służby podległe Ministrowi SWiA systemy łączności pozwalały im na skuteczną komunikację odpowiadającą wymogom i zagrożeniom współczesności? 3. Czy wykorzystywane przez służby podległe Ministrowi SWiA systemy łączności były ze sobą kompatybilne i umożliwiały bezpieczną i skuteczną współpracę pomiędzy formacjami w sytuacji kryzysowej?
Zakres podmiotowy	Kontrolą P/24/033 <i>Funkcjonowanie systemu łączności w służbach podległych MSWiA</i> zostało objętych 30 podmiotów, w tym: Ministerstwo Spraw Wewnętrznych i Administracji jako urząd realizujący zadania Ministra odpowiedzialnego za ochronę bezpieczeństwa państwa i porządku publicznego oraz Komendę Główną Policji, Komendę Główną Państwowej Straży Pożarnej, Komendę Główną Straży Granicznej i Służbę Ochrony Państwa. Kontrolę przeprowadzono także w jednostkach organizacyjnych podległych KGP, KG PSP i KG SG, tj. pięciu komendach wojewódzkich Policji i siedmiu komendach powiatowych/miejskich Policji, czterech komendach wojewódzkich PSP i pięciu komendach miejskich/powiatowych PSP oraz czterech oddziałach SG.
Kryteria kontroli	Kontrolę przeprowadzono na podstawie art. 2 ust. 1 ustawy z dnia 23 grudnia 1994 r. o Najwyższej Izbie Kontroli, z uwzględnieniem kryteriów określonych w art. 5 ust. 1 tej ustawy, tj. legalności, gospodarności, celowości i rzetelności.
Okres objęty kontrolą	Od 1 stycznia 2022 r. do 31 października 2024 r. (z wykorzystaniem dowodów wytworzonych przed i po tym okresie, związanych z przedmiotem tej kontroli). Czynności kontrolne przeprowadzono

w okresie od 3 września do 6 grudnia 2024 r. Kontrolę zakończono 30 grudnia 2024 r. (data podpisania ostatniego wystąpienia).

Kontrola rozpoznawcza	Niniejsza kontrola została poprzedzona kontrolą rozpoznawczą R/24/001 <i>Funkcjonowanie systemu łączności w służbach zlokalizowanych w m. st. Warszawie</i> , którą Departament Porządku i Bezpieczeństwa Wewnętrznego przeprowadził w czerwcu i lipcu 2024 r. w trzech jednostkach organizacyjnych: Komendzie Stołecznej Policji, Komendzie Wojewódzkiej Państwowej Straży Pożarnej w Warszawie i Nadwiślańskim Oddziale Straży Granicznej.
Działania na podstawie art. 29 ustawy o NIK	W ramach postępowania kontrolnego pozyskano, na podstawie art. 29 ust. 1 pkt 2 lit. f ustawy o NIK, informacje i dokumenty od Instytutu Łączności – Państwowego Instytutu Badawczego dotyczące zagadnień objętych kontrolą, tj. systemów łączności radiowej. Ponadto wsparcia merytorycznego w kontroli udzielił ekspert w zakresie specjalistycznej wiedzy o funkcjonowaniu systemów łączności radiowej, który konsultował m.in. techniczne i organizacyjne rozwiązania przyjęte w kontrolowanych podmiotach.
Badania kwestionariuszowe	NIK przeprowadziła badanie ankietowe skierowane do funkcjonariuszy służb podległych MSWiA dotyczące ich doświadczeń i opinii o środkach łączności radiowej oraz użytkowanych systemach. Na pytania zawarte w kwestionariuszu – aktywnym w okresie od 19 grudnia 2024 r. do końca stycznia 2025 r., który udostępniono zainteresowanym ze wsparciem zarządów mundurowych związków zawodowych, odpowiedzi udzieliło 119 funkcjonariuszy Policji i Państwowej Straży Pożarnej (ponad dwie trzecie respondentów to policjanci). Wyniki badania pokazały, że blisko połowa ankietowanych (49 proc.) korzysta w służbie z analogowych systemów łączności radiowej, a jedynie co piąty funkcjonariusz (22 proc.) użytkuje nowoczesny system cyfrowy w standardzie TETRA (ok. ¼ odpowiedzi wskazywała na brak wiedzy o systemie). Niemal wszyscy respondenci dostrzegają wady środków łączności radiowej, wśród których najczęściej wymieniano (możliwość wielokrotnego wyboru) ograniczenia techniczne jak: niewystarczający zasięg (83 proc. odpowiedzi), zła jakość połączenia (67 proc.), brak możliwości przesyłania plików (np. zdjęć) – 49 proc., a także kwestie systemowe, jak brak możliwości współpracy z innymi służbami (44 proc.). Całościowa ocena systemu łączności potwierdza, że dla ponad 80 proc. ankietowanych nie spełnia on (lub raczej nie spełnia) oczekiwań co do zasięgu na obszarze działania, a na brak funkcji przesyłania plików z danymi (zdjęć) wskazuje ponad 85 proc. odpowiadających. Także brak

możliwości nawiązania łączności z innymi służbami jest – dla trzech na czterech ankietowanych – powodem niskiej oceny systemu. Należy zauważyć, że funkcjonariusze doceniają wygodę korzystania z radiotelefonu i jego niezawodność – w tym obszarze wystąpiła niewielka przewaga pozytywnych odpowiedzi nad krytycznymi.

Wskazane wyżej trudności w użytkowaniu środków łączności uzupełniają informacje blisko 97 proc. ankietowanych o sytuacji/potrzebie posługiwania się w służbie prywatnym telefonem komórkowym, z uwagi m.in. na: brak możliwości połączenia przez radiotelefon z innym funkcjonariuszem ze swojej formacji (82 proc. wskazań), a także lepszą jakość połączenia i możliwość wykorzystania brakujących w radiotelefonie funkcji (np. nawigacji) – podobne wyniki, ok. 74 proc. odpowiedzi.

Zainteresowanie optymalnym rozwiązaniem hybrydowym wyraziło blisko 90 proc. respondentów, którzy dostrzegają potrzebę zastąpienia typowego radiotelefonu urządzeniem zbliżonym funkcjonalnością do tzw. smartfona, które umożliwiałoby zarówno służbową łączność radiową, jak i przesyłanie danych (zdjęcia, plany).

Pozostałe informacje

W kontroli koordynowanej przez Departament Porządku i Bezpieczeństwa Wewnętrznego NIK uczestniczyło pięć delegatur Najwyższej Izby Kontroli: w Katowicach, Olsztynie, Rzeszowie, Szczecinie i Warszawie. Wyniki kontroli przedstawiono w 30 wystąpieniach pokontrolnych, w których sformułowano ogółem 18 wniosków pokontrolnych. Ujawnione w trakcie kontroli nieprawidłowości nie miały wymiaru finansowego.

Najważniejsze wnioski skierowane zostały do Ministra SWiA i szefów służb podległych MSWiA, w tym dotyczące koordynacji i wdrożenia jednolitego systemu trankingowej łączności radiowej (przedstawiono je na str. 19 informacji). Pozostałe wnioski dotyczyły m.in. terminowej realizacji przeglądów stanu technicznego masztów antenowych, dostosowania norm należności sprzętu radiokomunikacyjnego do rzeczywistych potrzeb jednostek i uzupełnienia niedoborów środków łączności.

Kierownicy jednostek objętych kontrolą nie zgłosili zastrzeżeń do wystąpień pokontrolnych. Z ich odpowiedzi o sposobie realizacji wniosków pokontrolnych wynika, że na dzień 12 marca 2025 r. zrealizowano sześć wniosków, siedem jest w trakcie realizacji, a pięć nie zostało dotychczas zrealizowanych.

Wykaz jednostek
kontrolowanych

Lp.	Jednostka organizacyjna NIK przeprowadzająca kontrolę	Nazwa jednostki kontrolowanej	Imię i nazwisko kierownika jednostki kontrolowanej
1.	Departament Porządku i Bezpieczeństwa Wewnętrznego	Ministerstwo Spraw Wewnętrznych i Administracji	Tomasz Siemoniak
2.	Departament Porządku i Bezpieczeństwa Wewnętrznego	Komenda Główna Policji	nadinsp. Marek Boroń
3.	Departament Porządku i Bezpieczeństwa Wewnętrznego	Komenda Główna Państwowej Straży Pożarnej	nadbryg. dr inż. Mariusz Feltynowski
4.	Departament Porządku i Bezpieczeństwa Wewnętrznego	Komenda Główna Straży Granicznej	gen. dyw. SG Robert Bagan
5.	Departament Porządku i Bezpieczeństwa Wewnętrznego	Służba Ochrony Państwa	gen. bryg. SOP Radosław Jaworski
6.	Delegatura w Katowicach	Komenda Wojewódzka Policji w Katowicach	nadinsp. Mariusz Krzystyniak
7.	Delegatura w Katowicach	Komenda Wojewódzka PSP w Katowicach	nadbryg. Wojciech Kruczek
8.	Delegatura w Katowicach	Śląski Oddział SG w Raciborzu	gen. bryg. SG Andrzej Jakubaszek
9.	Delegatura w Katowicach	Komenda Powiatowa Policji w Raciborzu	podinsp. Marek Ryszka
10.	Delegatura w Katowicach	Komenda Powiatowa PSP w Raciborzu	st. bryg. Jarosław Ceglarek
11.	Delegatura w Olsztynie	Komenda Wojewódzka Policji w Olsztynie	insp. Miroslaw Elszkowski
12.	Delegatura w Olsztynie	Komenda Wojewódzka PSP w Olsztynie	nadbryg. Michał Kamieniecki
13.	Delegatura w Olsztynie	Warmińsko-Mazurski Oddział SG w Kętrzynie	ppłk SG Daniel Wojtaszkiewicz
14.	Delegatura w Olsztynie	Komenda Powiatowa Policji w Ostródzie	insp. Adam Borowski
15.	Delegatura w Olsztynie	Komenda Powiatowa PSP w Ostródzie	mł. bryg. Rafał Napiórkowski
16.	Delegatura w Rzeszowie	Komenda Wojewódzka Policji w Rzeszowie	insp. Jarosław Tokarczyk
17.	Delegatura w Rzeszowie	Komenda Wojewódzka PSP w Rzeszowie	st. bryg. Tomasz Baran
18.	Delegatura w Rzeszowie	Bieszczadzki Oddział SG w Przemyśle	gen. bryg. SG Tomasz Zybiński
19.	Delegatura w Rzeszowie	Komenda Miejska Policji w Rzeszowie	insp. Bogusław Kania

20.	Delegatura w Rzeszowie	Komenda Miejska PSP w Rzeszowie	st. bryg. Andrzej Wantrych
21.	Delegatura w Szczecinie	Komenda Wojewódzka Policji w Szczecinie	insp. Szymon Sędzik
22.	Delegatura w Szczecinie	Komenda Wojewódzka PSP w Szczecinie	st. bryg. Miroslaw Pender
23.	Delegatura w Szczecinie	Morski Oddział SG w Gdańsku	kontradm. SG Andrzej Prokopski
24.	Delegatura w Szczecinie	Komenda Miejska Policji w Świnoujściu	insp. Jarosław Czaja
25.	Delegatura w Szczecinie	Komenda Miejska PSP w Świnoujściu	st. kpt. Marek Wieczorek
26.	Delegatura w Warszawie	Komenda Wojewódzka Policji z/s w Radomiu	nadkom. Waldemar Wołowiec
27.	Delegatura w Warszawie	Komenda Powiatowa Policji w Grójcu	insp. Sławomir Rek
28.	Delegatura w Warszawie	Komenda Powiatowa Policji w Legionowie	nadkom. Zbigniew Pucelak
29.	Delegatura w Warszawie	Komenda Rejonowa Policji Warszawa I	insp. Marek Żyra
30.	Delegatura w Warszawie	Komenda Miejska PSP m.st. Warszawy	st. bryg. mgr inż. Roman Krzywiec

6.1.1. WYKAZ OCEN KONTROLOWANYCH JEDNOSTEK

Lp.	Nazwa jednostki kontrolowanej	Ocena kontrolowanej działalności ^{*/}	Stany mające wpływ na wydaną ocenę:	
			prawidłowe	nieprawidłowe
1.	Ministerstwo Spraw Wewnętrznych i Administracji	w formie opisowej	działania ustawowe dla wdrożenia systemu SBŁP	zwłoka, brak nadzoru nad wdrożeniem jednolitego systemu
2.	Komenda Główna Policji	w formie opisowej	organizacja łączności radiowej m.in. w standardzie cyfrowym	zróżnicowanie i ograniczenia systemów łączności, brak kompatybilności
3.	Komenda Główna Państwowej Straży Pożarnej	w formie opisowej	organizacja sprawnej łączności analogowej	ograniczenia systemu łączności, brak kompatybilności
4.	Komenda Główna Straży Granicznej	w formie opisowej	wdrożenie cyfrowej łączności radiowej	brak kompatybilności
5.	Służba Ochrony Państwa	w formie opisowej	sprawna łączność poprzez system cyfrowy i sieci analogowe	ograniczenia systemu łączności, brak kompatybilności
6.	Komenda Wojewódzka Policji w Katowicach	w formie opisowej	zapewnienie łączności w działaniach, z użyciem wielu systemów	zróżnicowanie i ograniczenia systemów łączności, brak kompatybilności
7.	Komenda Wojewódzka PSP w Katowicach	w formie opisowej	organizacja sprawnej podstawowej łączności	ograniczenia analogowej sieci łączności, brak kompatybilności
8.	Śląski Oddział SG w Raciborzu	w formie opisowej	sprawne działanie łączności cyfrowej	brak kompatybilności
9.	Komenda Powiatowa Policji w Raciborzu	w formie opisowej	zapewnienie sprawnej podstawowej łączności	ograniczenia analogowej sieci łączności, brak kompatybilności
10.	Komenda Powiatowa PSP w Raciborzu	w formie opisowej	zapewnienie sprawnej podstawowej łączności	ograniczenia analogowej sieci łączności, brak kompatybilności

11.	Komenda Wojewódzka Policji w Olsztynie	w formie opisowej	zapewnienie prowadzenie działań z użyciem wielu systemów	zróżnicowanie i ograniczenia systemów łączności, brak kompatybilności
12.	Komenda Wojewódzka PSP w Olsztynie	w formie opisowej	organizacja sprawnej podstawowej łączności	ograniczenia analogowej sieci łączności, brak kompatybilności
13.	Warmińsko-Mazurski Oddział SG w Kętrzynie	pozytywna	sprawne działanie łączności cyfrowej w standardzie DMR	brak kompatybilności z innymi służbami
14.	Komenda Powiatowa Policji w Ostródzie	w formie opisowej	zapewnienie sprawnej podstawowej łączności	ograniczenia analogowej sieci łączności, brak kompatybilności
15.	Komenda Powiatowa PSP w Ostródzie	w formie opisowej	zapewnienie sprawnej podstawowej łączności	ograniczenia analogowej sieci łączności, brak kompatybilności
16.	Komenda Wojewódzka Policji w Rzeszowie	w formie opisowej	zapewnienie łączności w działaniach, z użyciem wielu systemów	zróżnicowanie i ograniczenia systemów łączności, brak kompatybilności
17.	Komenda Wojewódzka PSP w Rzeszowie	w formie opisowej	zapewnienie sprawnej podstawowej łączności	ograniczenia analogowej sieci łączności, brak kompatybilności
18.	Bieszczadzki Oddział SG w Przemyśle	w formie opisowej	sprawne działanie łączności cyfrowej	brak kompatybilności
19.	Komenda Miejska Policji w Rzeszowie	w formie opisowej	zapewnienie sprawnej podstawowej łączności	ograniczenia analogowej sieci łączności, brak kompatybilności
20.	Komenda Miejska PSP w Rzeszowie	w formie opisowej	zapewnienie sprawnej podstawowej łączności	ograniczenia analogowej sieci łączności, brak kompatybilności
21.	Komenda Wojewódzka Policji w Szczecinie	w formie opisowej	zapewnienie łączności w działaniach, z użyciem wielu systemów	zróżnicowanie i ograniczenia systemów łączności, brak kompatybilności
22.	Komenda Wojewódzka PSP w Szczecinie	w formie opisowej	zapewnienie sprawnej podstawowej łączności	ograniczenia analogowej sieci łączności, brak kompatybilności

23.	Morski Oddział SG w Gdańsku	w formie opisowej	sprawne działanie łączności cyfrowej	brak kompatybilności
24.	Komenda Miejska Policji w Świnoujściu	w formie opisowej	zapewnienie sprawnej podstawowej łączności	ograniczenia analogowej sieci łączności, brak kompatybilności
25.	Komenda Miejska PSP w Świnoujściu	w formie opisowej	zapewnienie sprawnej podstawowej łączności	ograniczenia analogowej sieci łączności, brak kompatybilności
26.	Komenda Wojewódzka Policji z/s w Radomiu	w formie opisowej	zapewnienie łączności w działaniach, z użyciem wielu systemów	zróżnicowanie i ograniczenia systemów łączności, brak kompatybilności
27.	Komenda Powiatowa Policji w Grójcu	w formie opisowej	zapewnienie sprawnej podstawowej łączności	ograniczenia analogowej sieci łączności, brak kompatybilności
28.	Komenda Powiatowa Policji w Legionowie	w formie opisowej	zapewnienie sprawnej podstawowej łączności	ograniczenia analogowej sieci łączności, brak kompatybilności
29.	Komenda Rejonowa Policji Warszawa I	w formie opisowej	zapewnienie sprawnej łączności radiowej TETRA	brak kompatybilności z innymi służbami
30.	Komenda Miejska PSP m.st. Warszawy	w formie opisowej	zapewnienie sprawnej podstawowej łączności	ograniczenia analogowej sieci łączności, brak kompatybilności

*/ pozytywna / w formie opisowej / negatywna

6.2. ANALIZA STANU PRAWNEGO I UWARUNKOWAŃ ORGANIZACYJNO-EKONOMICZNYCH

Nowa ustawa o ochronie ludności i obronie cywilnej

Istotnym elementem stanu prawnego w obszarze zapewnienia skutecznej łączności radiowej między służbami podległymi MSWiA stała się ustawa z dnia 5 grudnia 2024 r. o ochronie ludności i obronie cywilnej (Dz. U. poz. 1907), która weszła w życie w dniu 1 stycznia 2025 r. Regulacja ta porządkuje działania i obowiązki podmiotów ochrony ludności dotyczące reagowania w czasie pokoju, stanu wojennego i wojny, przy tym koncentruje się na bezpieczeństwie obywateli, co odpowiada społecznym potrzebom wobec potencjalnych zagrożeń militarnych i pozamilitarnych. Ustawa wypełniła lukę prawną w zakresie funkcjonowania obrony cywilnej, którą spowodowało wejście w życie ustawy z 11 marca 2022 r. o obronie Ojczyzny.

Dla zapewnienia ciągłości funkcjonowania administracji państwowej oraz ochrony ludności w czasie pokoju i w czasie wojny, w ustawie określono zadania w zakresie wykrywania zagrożeń, ostrzegania, powiadamiania i alarmowania o zagrożeniach oraz utworzenia Systemu Bezpiecznej Łączności Państwowej (SBŁP), zorganizowanego i nadzorowanego przez ministra właściwego do spraw wewnętrznych – operatora systemu. System będzie funkcjonował na kanałach łączności w sieci stacjonarnej, radiowej, komórkowej i satelitarnej, a w perspektywie do 2030 r. ma umożliwić zbudowanie interoperacyjności pomiędzy systemami łączności i komunikacji administracji publicznej, służb mundurowych podległych MSWiA z systemami użytkowanymi w jednostkach MON.

Ramy organizacji łączności w służbach

Minister Spraw Wewnętrznych i Administracji jest naczelnym organem administracji państwowej odpowiedzialnym za ochronę bezpieczeństwa państwa i porządku publicznego oraz sprawuje nadzór nad służbami: Policją, Strażą Graniczną, Służbą Ochrony Państwa oraz Państwową Strażą Pożarną. Podejmowane w MSWiA od lat działania w celu zorganizowania nowoczesnego i jednolitego systemu łączności radiowej dla podległych służb nie przyniosły dotąd rzeczywistego efektu – każda formacja wdrożyła autonomiczny system łączności radiowej i ustaliła ramy jego działania. Wyznaczony w MSWiA do m.in. rozwoju i koordynacji oraz wykorzystania sieci i systemów radiokomunikacyjnych dla Ministra i jednostek mu podległych Departament Teleinformatyki realizował głównie zadanie zapewnienia zasobów częstotliwości radiowych dla sieci i systemów radiokomunikacyjnych służb MSWiA.

Komendant Główny Policji określił, w zarządzeniu nr 22 z 14 lipca 2020 r. *w sprawie określenia metod i form wykonywania zadań Policji z użyciem środków łączności radiowej*, organizację łączności radiowej Policji i współdziałanie z pozapolicyjnymi sieciami łączności, stosowanie środków

łączności i sposób prowadzenia korespondencji radiowej. Funkcjonujące w Policji systemy są niejednorodne, oparte na różnych standardach ETSI. Aktualnie trwa wdrażanie do eksploatacji w kolejnych jednostkach Policji systemu radiokomunikacyjnego Policji TETRA (SRP-T) na mocy decyzji Dyrektora Biura Łączności i Informatyki KGP z 2 sierpnia 2022 r. Zarządzenie nr 27 KGP z 16 kwietnia 2019 r. ustaliło normy wyposażenia w sprzęt łączności radiowej, satelitarnej i przewodowej przysługujące jednostkom organizacyjnym Policji oraz policjantom, na podstawie którego opracowane zostały tabele należności sprzętu łączności.

Komendant Główny Straży Granicznej uregulował organizację i sposób funkcjonowania systemu łączności w SG zarządzeniem nr 33 z dnia 2 sierpnia 2011 r. w *sprawie łączności radiowej w systemach ultrakrótkofalowej łączności radiowej przy wykonywaniu zadań w jednostkach organizacyjnych Straży Granicznej*. Określono w nim zasady stosowania środków łączności radiowej, sposób organizacji łączności radiowej oraz sposób prowadzenia korespondencji radiowej. Dyrektor Biura Łil KGSG jako upoważniony do wydawania decyzji, instrukcji, wytycznych, poleceń w sprawach łączności, wydał dalsze regulacje w zakresie łączności radiowej w jednostkach SG, w tym wytyczne do programowania urządzeń radiowych standardu DMR.

Komendant Główny PSP uregulował zasady łączności radiowej w instrukcji wprowadzonej w kwietniu 2019 r., która opisuje: zasady stosowania środków łączności radiowej, organizację łączności radiowej, prowadzenia dokumentacji, realizacji szkoleń oraz sposób prowadzenia korespondencji radiowej w jednostkach ochrony przeciwpożarowej. W Instrukcji określono też zasady budowy sieci radiowych, wymagania technicznofunkcyjne dla radiotelefonów i instalacji antenowych, zasady programowania radiotelefonów, zasady tworzenia kryptonimów, zasady prowadzenia korespondencji radiowej, wymagania stawiane abonentom sieci radiowych oraz dokumentację łączności.

Komendant Służby Ochrony Państwa decyzją nr 116/2018 z 2 maja 2018 r. wprowadził procedury eksploatacji urządzeń łączności, która obejmuje m.in. zasady instalacji sprzętu łączności radiowej w obiektach i pojazdach służbowych SOP oraz na potrzeby działań ochronnych, obsługę środków łączności radiowej (programowanie, przeglądy i serwisowanie). Organizację łączności radiowej regulują także decyzje i zarządzenia dotyczące np. wymagań w zakresie organizacji łączności grup ochrony bezpośredniej.

6.3. WYKAZ AKTÓW PRAWNYCH DOTYCZĄCYCH KONTROLOWANEJ DZIAŁALNOŚCI

1. Ustawa z dnia 5 grudnia 2024 r. o ochronie ludności i obronie cywilnej (Dz. U. poz. 1907).
2. Ustawa z dnia 6 kwietnia 1990 r. o Policji (Dz. U. z 2024 r. poz. 145, ze zm.).
3. Ustawa z dnia 12 października 1990 r. o Straży Granicznej (Dz. U. z 2024 r. poz. 915, ze zm.).
4. Ustawa z dnia 24 sierpnia 1991 r. o Państwowej Straży Pożarnej (Dz. U. z 2024 r. poz. 1443, ze zm.)
5. Ustawa o Służbie Ochrony Państwa z dnia 8 grudnia 2017 roku (Dz. U. z 2025 r. poz. 34).
6. Ustawa z dnia 11 marca 2022 r. o obronie Ojczyzny (Dz. U. z 2024 r. poz. 248, ze zm.)
7. Ustawa z dnia 21 czerwca 1996 r. o szczególnych formach sprawowania nadzoru przez ministra właściwego do spraw wewnętrznych (Dz.U. z 2024 r., poz. 309, ze zm.).
8. Ustawa z dnia 17 grudnia 2021 r. o ustanowieniu „Programu modernizacji Policji, Straży Granicznej, Państwowej Straży Pożarnej i Służby Ochrony Państwa w latach 2022–2025”, o ustanowieniu "Programu modernizacji Służby Więziennej w latach 2022–2025" oraz o zmianie ustawy o Policji i niektórych innych ustaw (Dz.U. z 2024 r., poz.86).
9. Zarządzenie nr 22 Komendanta Głównego Policji z dnia 14 lipca 2020 r. w sprawie określania metod i form wykonywania zadań Policji z użyciem środków łączności radiowej (Dz. Urz. KGP z 2020 r. poz. 38, ze zm.).
10. Zarządzenie nr 27 Komendanta Głównego Policji z dnia 16 kwietnia 2019 r. w sprawie określenia norm wyposażenia jednostek i komórek organizacyjnych Policji oraz funkcjonariuszy i pracowników Policji w sprzęt teleinformatyczny i telekomunikacyjny oraz szczegółowych zasad jego przyznawania i użytkowania (Dz. Urz. KGP poz. 66, ze zm.).
11. Zarządzenie Nr 33 Komendanta Głównego Straży Granicznej z dnia 2 sierpnia 2011 r. w sprawie łączności radiowej w systemach ultrakrótkofalowej łączności radiowej przy wykonywaniu zadań w jednostkach organizacyjnych Straży Granicznej (Dz. Urz. KGSG Nr 9, poz. 36).

12. Normy ETSI TS 102 361 część 1 – 4, które definiują specyfikacje techniczne dla systemów Digital Mobile Radio (DMR) stosowane w łączności radiowej (<https://www.etsi.org>).

6.4. WYKAZ PODMIOTÓW, KTÓRYM PRZEKAZANO INFORMACJĘ O WYNIKACH KONTROLI

1. Prezydent Rzeczypospolitej Polskiej
2. Marszałek Sejmu Rzeczypospolitej Polskiej
3. Marszałek Senatu Rzeczypospolitej Polskiej
4. Prezes Rady Ministrów
5. Prezes Trybunału Konstytucyjnego
6. Rzecznik Praw Obywatelskich
7. Przewodniczący Komisji do Spraw Kontroli Państwowej Sejmu RP
8. Przewodniczący Komisji Administracji i Spraw Wewnętrznych Sejmu RP
9. Przewodniczący Senackiej Komisji Samorządu Terytorialnego i Administracji Państwowej
10. Minister Spraw Wewnętrznych i Administracji
11. Komendant Główny Policji
12. Komendant Główny Państwowej Straży Pożarnej
13. Komendant Główny Straży Granicznej
14. Komendant Służby Ochrony Państwa



Minister Spraw Wewnętrznych i Administracji

DK-KKN.096.1.16.2025

Warszawa, /elektroniczny znacznik czasu/

Pan
Marian Banaś
Prezes
Najwyższej Izby Kontroli

Szanowny Panie Prezesie

zgodnie z art. 64 ust. 2 ustawy z dnia 23 grudnia 1994 r. o Najwyższej Izbie Kontroli¹ przekazuję stanowisko do Informacji o wynikach kontroli P/24/033 – Funkcjonowanie systemu łączności w służbach podległych MSWiA.

Ad 1

Pilne wdrożenie jednolitego systemu cyfrowej łączności radiowej poprzez:

- a) zapewnienie skutecznej koordynacji i priorytetowego traktowania działań na rzecz budowy Systemu Bezpiecznej Łączności Państwowej (SBŁP), w tym w tym jego podsystemu radiowej łączności trankingowej (SBŁP-T), jako kluczowego elementu zapewnienia bezpieczeństwa i interoperacyjności służb,***
- b) ograniczenie rozwoju niekompatybilnych systemów łączności i zapewnienie spójnego podejścia do budowy infrastruktury radiowej w służbach podległych MSWiA.***

Celem realizacji ww. zaleceń planowane jest powołanie Zespołu do wypracowania rozwiązań organizacyjnych i funkcjonalno - technicznych oraz pozostałych wymagań i warunków związanych z budową, utrzymaniem oraz rozwojem Systemu Bezpiecznej Łączności Państwowej.

Ograniczenie rozwoju niekompatybilnych systemów łączności i zapewnienie spójnego podejścia do budowy infrastruktury radiowej w służbach podległych MSWiA będzie odbywało się poprzez opiniowanie rozwiązań radiokomunikacyjnych planowanych do wdrażania w służbach resortu spraw wewnętrznych i administracji w ramach nadzoru prowadzonego przez MSWiA.

Ad 2

Opracowanie perspektywicznego modelu działania systemu cyfrowej łączności radiowej uwzględniającego rozwój nowych technologii, w tym m.in. umożliwiających w czasie rzeczywistym lokalizację używanych sił i środków oraz zarządzanie operacjami przy pomocy obrazowania obszaru objętego działaniem, a także integrację z systemami IT, w szczególności w zakresie cyberbezpieczeństwa.

Planuje się uwzględnienie przedmiotowego zalecenia w ramach prac nad Systemem Bezpiecznej Łączności Państwowej w kontekście systemu łączności krytycznej Unii Europejskiej (EU Critical Communication System – EUCCS),

¹ t.j. Dz. U. z 2022 r. poz. 623

łączącego systemy łączności krytycznej nowej generacji państw członkowskich w UE.

Należy przy tym wspomnieć, że w dniu 1 kwietnia br. Komisja Europejska wydała komunikat w sprawie ProtectEU: europejskiej strategii bezpieczeństwa wewnętrznego (COM(2025)148). Jednym z elementów tej strategii jest łączność krytyczna. Planowane jest zbudowanie systemu łączności krytycznej Unii Europejskiej (EU Critical Communication System – EUCCS), łączącego systemy łączności krytycznej nowej generacji państw członkowskich w UE. EUCCS będzie opierał się na trzech filarach strategicznych: mobilności operacyjnej, dużej odporności i autonomii strategicznej. Wykorzystanie przyszłego wieloorbitalnego systemu IRIS² zapewni rozszerzenie zasięgu tego systemu. Dedykowana temu zagadnieniu grupa robocza Mission Critical Communication Group (MCCG), w której pracach udział biorą także przedstawiciele MSWiA, opracowała Plan operacyjny dla rozwoju EUCCS. Plan ten został przesłany do dalszego procedowania do Parlamentu Europejskiego, a jego przyjęcie przewidywane jest na przełomie 2025 i 2026 roku.

W kontekście powyższych planów KE, w związku z potrzebą powołania w Polsce jednostki zarządzającej dla komunikacji krytycznej, tzw. Competent Critical Communication Authority (CCCA), biorąc pod uwagę rekomendacje KE, aby przy powołaniu CCCA wykorzystać doświadczenie i zasoby ludzkie z jednostek zarządzających innymi programami i usługami, oraz biorąc pod uwagę fakt, że usługi GOVSATCOM będą jednym z elementów systemu komunikacji krytycznej, Sekretarz Stanu w MSWiA, zaaprobował dołączenie przepisów regulujących powołanie CCCA do obecnie przygotowywanego w MSWiA projektu ustawy o jednostkach zarządzających GOVSATCOM i Secure Connectivity i rozpoczęcie prac w zakresie przygotowania krajowej strategii komunikacji krytycznej.

W związku z powyższym zagadnienia dotyczące łączności radiowej, w szczególności rozpatrywanie perspektywicznego modelu działania systemu cyfrowej łączności radiowej uwzględniającego rozwój nowych technologii, w tym m.in. umożliwiających w czasie rzeczywistym lokalizację używanych sił i środków oraz zarządzanie operacjami przy pomocy obrazowania obszaru objętego działaniem, a także integrację z systemami IT, w szczególności w zakresie cyberbezpieczeństwa, będzie rozpatrywane w kontekście udziału Polski w EUCCS.

Ad 3

Podjęcie przez Ministra SWiA w porozumieniu z ministrem właściwym do spraw informatyzacji skutecznych działań mających na celu włączenia PSP do katalogu podmiotów uprawnionych do korzystania ze świadczenia teleinformatycznego określonego w art. 5 ustawy z dnia 2 grudnia 2021 r. o szczególnych zasadach wynagradzania osób realizujących zadania z zakresu cyberbezpieczeństwa.

W Ministerstwie Spraw Wewnętrznych i Administracji podjęto działania w celu realizacji ww. wniosku. Propozycja dot. włączenia PSP do katalogu podmiotów uprawnionych do korzystania ze świadczenia teleinformatycznego określonego w art. 5 ustawy z dnia 2 grudnia 2021 r. o szczególnych zasadach wynagradzania osób realizujących zadania z zakresu cyberbezpieczeństwa została zgłoszona przez MSWiA w ramach prac nad projektem ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32).

Projekt ww. ustawy, który w lutym br., został przyjęty przez Komitet do spraw Europejskich zawiera m.in. zmiany przepisów w zakresie:

- **ustawy z dnia 24 sierpnia 1991 r. o Państwowej Straży Pożarnej²**, do której wprowadza się następujące zmiany: w art. 93 w ust. 1 dodaje się pkt 8 w brzmieniu:
„8) świadczenie teleinformatyczne, o którym mowa w art. 5 ustawy z dnia 2 grudnia 2021 r. o szczególnych zasadach wynagradzania osób realizujących zadania z zakresu cyberbezpieczeństwa (Dz. U. z 2023 r. poz. 667, z późn. zm.), zwane dalej "świadczeniem teleinformatycznym".;
po art. 97f dodaje się art. 97g w brzmieniu:
„Art. 97g. 1. Strażakowi wykonującemu zadania z zakresu cyberbezpieczeństwa, o których mowa w art. 26, art. 42 ust. 1, art. 44 ust. 1, art. 62 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2024 r. poz. 1077 i 1222), lub w zakresie zapewnienia cyberbezpieczeństwa w Państwowej Straży Pożarnej przyszanje się na okres ich wykonywania świadczenie teleinformatyczne....
- **ustawy z dnia 2 grudnia 2021 r. o szczególnych zasadach wynagradzania osób realizujących zadania z zakresu cyberbezpieczeństwa³**, do której wprowadza się następujące zmiany m.in. w art. 5:
 - a) pkt 1 otrzymuje brzmienie:
 - „1) w CSIRT MON, CSIRT NASK, CSIRT GOV, CSIRT sektorowych, organach właściwych do spraw cyberbezpieczeństwa lub w urzędzie obsługującym Pełnomocnika Rządu do Spraw Cyberbezpieczeństwa, o których mowa odpowiednio w art. 26, art. 41, art. 44 lub art. 60 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa;”,
 - b) w pkt 2 w lit. n dodaje się przecinek i dodaje się lit. o-r w brzmieniu:
 - „o) Urzędzie Ochrony Danych Osobowych,
 - p) jednostkach organizacyjnych Krajowej Administracji Skarbowej, o których mowa w art. 36 ust. 1 pkt 3 i 5 ustawy dnia 16 listopada 2016 r. o Krajowej Administracji Skarbowej (Dz. U. z 2023 r. poz. 615, z późn. zm.),
 - r) Państwowej Straży Pożarnej.”

Reasumując, uwzględniono propozycję MSWiA dot. włączenia PSP do katalogu podmiotów uprawnionych do korzystania ze świadczenia teleinformatycznego.

Projekt ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32) według stanu na dzień 30 maja br. ma zostać skierowany w najbliższym czasie przez Ministerstwo Cyfryzacji na SKRM.

Ad 4

Wzmocnienie nadzoru nad funkcjonowaniem systemów łączności radiowej w służbach poprzez:

- a) **wprowadzenie mechanizmów systematycznego nadzoru nad funkcjonowaniem i rozwojem systemów łączności radiowej, w tym zapewnienie pełnej informacji o problemach operacyjnych,**

² Dz. U. z 2024 r. poz. 1443 i 1473

³ Dz. U. z 2023 r. poz. 667 oraz z 2024 r. poz. 834 i 1222

b) określenie w strukturze MSWiA odpowiedzialnych komórek organizacyjnych nadzorujących łączność radiową i zapewnienie im odpowiednich zasobów kadrowych i kompetencyjnych.

Biorąc pod uwagę wnioski zawarte w wystąpieniu pokontrolnym Najwyższej Izby Kontroli z przeprowadzonej kontroli P/24/033 *Funkcjonowanie systemu łączności w służbach podległych MSWiA*, zarządzeniem nr 5 z dnia 3 lutego 2025 r. *Ministra Spraw Wewnętrznych i Administracji* zmieniającym zarządzenie w sprawie ustalenia regulaminu organizacyjnego Ministerstwa Spraw Wewnętrznych i Administracji dokonano zmiany zarządzenia w sprawie ustalenia regulaminu organizacyjnego MSWiA⁴ i w ramach tego do katalogu zadań Departamentu Teleinformatyki MSWiA, zawartych w § 25 regulaminu wpisano zadanie: „1a) prowadzenie spraw związanych z nadzorem Ministra nad budową i wdrożeniem Systemu Bezpiecznej łączności Państwowej (SBŁP) w zakresie niezastrzeżonym dla Pełnomocnika Ministra Spraw Wewnętrznych i Administracji do spraw organizacji Systemu Bezpiecznej łączności Państwowej oraz Pełnomocnika Rządu do spraw Systemu Bezpiecznej łączności Państwowej, o którym mowa w art. 81 ustawy z dnia 5 grudnia 2024 r. o ochronie ludności i obronie cywilnej, oraz innych komórek organizacyjnych ministerstwa” oraz zadanie „1b) prowadzenie spraw związanych z nadzorem Ministra nad Policją, Strażą Graniczną, Państwową Strażą Pożarną i Służbą Ochrony Państwa, w zakresie funkcjonujących w nich systemów łączności radiowej, w zakresie niezastrzeżonym dla innych komórek organizacyjnych Ministerstwa, w tym:

- a) opiniowanie rozwiązań radiokomunikacyjnych planowanych do wdrażania w służbach resortu spraw wewnętrznych i administracji,
- b) opiniowanie planowanych wdrożeń sieci radiowych służących współdziałaniu pomiędzy poszczególnymi służbami resortu spraw wewnętrznych i administracji oraz planowanych wdrożeń sieci radiowych służących współdziałaniu danej służby resortu spraw wewnętrznych i administracji z innymi podmiotami realizującymi zadania z obszaru obronności, bezpieczeństwa państwa, bezpieczeństwa publicznego, porządku publicznego, ratownictwa i zarządzania kryzysowego, ochrony ludności i obrony cywilnej,
- c) kontrolowanie prawidłowości wykorzystywania przez poszczególne służby przydzielonych im zasobów częstotliwości radiowych”.

Obecnie trwają prace nad wprowadzeniem tych zadań do wewnętrznego regulaminu organizacyjnego Departamentu Teleinformatyki MSWiA.

Ponadto, w kontekście przypisania zadań nadzorczych Departamentowi Teleinformatyki MSWiA, niezbędnym jest jego wzmocnienie etatowe, zmierzające do odbudowy zasobów pracowniczych Wydziału Radiokomunikacji i Systemów Satelitarnych MSWiA (dalej: WRSS MSWiA) w obszarze stanowisk zajmujących się sprawami łączności radiowej. W wyniku przeprowadzonego w ostatnim czasie naboru, od 8 stycznia 2025 r. w ww. Wydziale zatrudniono jedną osobę, zajmującą się zagadnieniami dotyczącymi systemów i sieci radiokomunikacyjnych. Obecnie sprawami radiokomunikacji zajmuje się więc jeden pracownik oraz doraźnie naczelnik Wydziału. Ponadto, w maju 2025 roku rozpoczęto procedurę kolejnego naboru na stanowisko głównego specjalisty do spraw planowania sieci radiowych

⁴ Dz. Urz. MSWiA z 2023 r. poz. 40.

oraz gospodarowania zasobami częstotliwości i numeracji dla sieci i systemów radiokomunikacyjnych. Docelowo planowane jest, aby sprawami radiokomunikacji w WRSS MSWiA zajmowały się co najmniej 4 osoby.

Ad 5

Zapewnienie łączności radiowej służbom w budynkach o utrudnionej propagacji sygnału, poprzez przeprowadzenie analizy zasadności stosowania urządzeń retransmisji sygnału, a w razie potrzeby – opracowanie odpowiednich regulacji prawnych.

Zagadnienie dotyczące zapewnienie łączności radiowej służbom w budynkach o utrudnionej propagacji sygnału, jest złożonym zagadnieniem technicznym. W ramach realizacji tego zalecenia NIK zostanie przeprowadzona analiza zasadności stosowania urządzeń retransmisji sygnału, w aspekcie rozszerzenia funkcjonalności rozwiązań w ramach powstającego Systemu Bezpiecznej łączności Państwowej, np. w ramach prac Zespołu, o którym mowa w Ad 1. Nie można wykluczyć, pojawienia się konieczności wprowadzenia zmian w obowiązujących przepisach, w kontekście wymagań dla niektórych kategorii obiektów budowlanych.

Z poważaniem

z up. Ministra Spraw Wewnętrznych i Administracji

Tomasz Szymański

Sekretarz Stanu

(podpisano kwalifikowanym podpisem elektronicznym)