Warszawa, dnia 23 grudnia 2025 r.

Poz. 1859

ROZPORZĄDZENIE
RADY MINISTRÓW

z dnia 22 grudnia 2025 r.

w sprawie sposobu korzystania z Systemu Bezpiecznej Łączności Państwowej, minimalnych wymagań technicznych i funkcjonalnych oraz minimalnego poziomu bezpieczeństwa usług tego systemu

Na podstawie art. 78 ust. 2 ustawy z dnia 5 grudnia 2024 r. o ochronie ludności i obronie cywilnej (Dz. U. poz. 1907 oraz z 2025 r. poz. 1705) zarządza się, co następuje:

§ 1. Rozporządzenie określa:

1) sposób korzystania z Systemu Bezpiecznej Łączności Państwowej, zwanego dalej „SBŁP", przez podmioty, o których mowa w art. 76 ust. 1 ustawy z dnia 5 grudnia 2024 r. o ochronie ludności i obronie cywilnej, zwanej dalej „ustawą";

2) minimalne wymagania techniczne i funkcjonalne, jakie musi spełniać SBŁP;

3) minimalny poziom bezpieczeństwa usług transmisji danych, połączeń głosowych oraz wiadomości tekstowych świadczonych w ramach SBŁP.

§ 2. Użyte w rozporządzeniu określenia oznaczają:

1) organizator podsystemu – podmiot, któremu operator SBŁP, o którym mowa w art. 74 ust. 2 ustawy, zleca zadania związane z organizacją, budową, utrzymaniem i modernizacją podsystemu SBŁP w określonym zakresie;

2) użytkownik instytucjonalny – podmiot, o którym mowa w art. 76 ust. 1 ustawy, który faktycznie korzysta z usług SBŁP;

3) usługa SBŁP – niepubliczna usługa telekomunikacyjna spełniająca wymogi cyberbezpieczeństwa oraz zapewniająca możliwość szyfrowania komunikacji;

4) dokumentacja podsystemu SBŁP – opracowana przez organizatora danego podsystemu SBŁP i zatwierdzona przez operatora SBŁP dokumentacja określająca rozwiązania techniczne i funkcjonalne w zakresie infrastruktury SBŁP, sposób dostępu do danych w ramach podsystemu SBŁP i okres przechowywania tych danych na potrzeby zapewnienia rozliczalności, sposób zapewnienia bezpieczeństwa i odporności komunikacji, zakres odpowiedzialności organizatora podsystemu, administratora i użytkownika instytucjonalnego oraz zakres i sposób sprawowania audytu i kontroli przez operatora SBŁP lub na zlecenie operatora SBŁP;

5) infrastruktura SBŁP – urządzenia teleinformatyczne SBŁP wraz z urządzeniami zasilającymi i sieciami telekomunikacyjnymi w rozumieniu art. 2 pkt 58 ustawy z dnia 12 lipca 2024 r. – Prawo komunikacji elektronicznej (Dz. U. poz. 1221 oraz z 2025 r. poz. 637 i 820) oraz, jeżeli dokumentacja podsystemu SBŁP tak stanowi, wraz z urządzeniami końcowymi.

§ 3. 1. Podmioty, o których mowa w art. 76 ust. 1 ustawy, korzystają z poszczególnych usług SBŁP na podstawie zgody operatora SBŁP udzielonej na ich pisemny wniosek.

2. Korzystanie z usług SBŁP odbywa się w zakresie uprawnień przyznanych w zgodzie operatora SBŁP, o której mowa w ust. 1, zgodnie z ich przeznaczeniem oraz zgodnie z dokumentacją podsystemu SBŁP.

3. Użytkownik instytucjonalny zgłasza operatorowi SBŁP, za pośrednictwem organizatora podsystemu SBŁP, nieprawidłowości dotyczące świadczonej usługi SBŁP oraz przekazuje organizatorowi podsystemu SBŁP informacje niezbędne do zapewniania ciągłości działania usługi SBŁP.

4. W przypadku stwierdzenia zagrożenia naruszenia bezpieczeństwa informacji lub konieczności zachowania ciągłości usługi SBŁP organizator podsystemu SBŁP w uzgodnieniu z operatorem SBŁP może w zakresie niezbędnym i na czas konieczny do usunięcia zagrożenia czasowo ograniczyć lub zawiesić świadczenie usługi wobec danego użytkownika instytucjonalnego.

§ 4. Minimalne wymagania techniczne SBŁP obejmują:

1) stosowanie obowiązujących i adekwatnych specyfikacji technicznych w procesie doboru komponentów infrastruktury SBŁP;

2) wykorzystanie narzędzi i urządzeń kryptograficznych, w tym narzędzi i urządzeń certyfikowanych w rozumieniu przepisów o ochronie informacji niejawnych;

3) stosowanie wymogów cyberbezpieczeństwa oraz szyfrowania komunikacji w ramach usług SBŁP;

4) wykorzystywanie przez użytkownika instytucjonalnego wyłącznie urządzeń akceptowanych lub dostarczanych przez operatora SBŁP lub organizatora podsystemu SBŁP;

5) określenie w dokumentacji podsystemu SBŁP minimalnej dostępności usług SBŁP oraz ustalenie dopuszczalnych opóźnień w transmisji danych;

6) określenie w dokumentacji podsystemu SBŁP czasu zestawienia połączeń zapewniających odpowiednią jakość komunikacji oraz minimalizację opóźnień w przypadku połączeń głosowych;

7) priorytetyzację w zakresie realizowanych usług SBŁP, w szczególności związanych z alarmowaniem i ostrzeganiem ludności, działaniami ratowniczymi, również w warunkach przeciążenia sieci telekomunikacyjnych;

8) zapewnienie możliwie najszybszego dostarczenia wiadomości alarmowych, ostrzegawczych i skutecznego mechanizmu potwierdzenia ich doręczenia, o ile jest wymagane, oraz odczytu tych wiadomości.

§ 5. 1. W zakresie jawnej łączności stacjonarnej (podsystem SBŁP-J) zapewnia się usługi telekomunikacyjne o minimalnych funkcjonalnościach obejmujących:

1) usługę przesyłu danych (transmisja danych) o gwarantowanych parametrach jakości, w tym realizowaną jako wirtualne sieci prywatne (VPN);

2) usługę połączeń głosowych;

3) usługę poczty elektronicznej.

2. W zakresie niejawnej łączności stacjonarnej wykorzystującej urządzenia lub narzędzia kryptograficzne (podsystem SBŁP-N) zapewnia się usługi telekomunikacyjne o minimalnych funkcjonalnościach obejmujących:

1) usługę przesyłu danych niejawnych (transmisja danych) o gwarantowanych parametrach jakości, w tym realizowaną jako wirtualne sieci prywatne (VPN);

2) usługę połączeń głosowych;

3) usługę poczty elektronicznej.

3. W zakresie wielopunktowej wideokonferencji (podsystem SBŁP-V) zapewnia się usługę telekomunikacyjną o minimalnych funkcjonalnościach obejmujących usługę transmisji audio-wideo, w tym realizowaną z wykorzystaniem urządzeń lub narzędzi kryptograficznych oraz dedykowanych systemów mostków konferencyjnych, odseparowanych od sieci publicznych, gwarantujących przetwarzanie komunikacji wyłącznie na terytorium Rzeczypospolitej Polskiej.

4. W zakresie bezpiecznej łączności mobilnej (podsystem SBŁP-M) zapewnia się usługi telekomunikacyjne o minimalnych funkcjonalnościach obejmujących:

1) w zakresie łączności mobilnej jawnej świadczonej w sposób zapewniający interoperacyjność z bezpieczną radiową łącznością trankingową:

   a) usługę jawnych połączeń głosowych,

   b) usługę jawnej transmisji danych, w tym na potrzeby przesyłania obrazów, wideo i danych telemetrycznych wykorzystującą urządzenia lub narzędzia kryptograficzne,

   c) usługę wymiany jawnych wiadomości tekstowych (SMS/RCS),

   d) usługę dostępu do internetu spełniającą wymogi cyberbezpieczeństwa oraz zapewniającą możliwość szyfrowania komunikacji;

2) w zakresie łączności mobilnej niejawnej komórkowej przy wykorzystaniu urządzeń lub narzędzi kryptograficznych:

a) usługę wymiany niejawnych wiadomości tekstowych,

b) usługę niejawnych połączeń głosowych,

c) usługę niejawnej transmisji danych, w tym na potrzeby przesyłania obrazów i wideo,

d) usługę niejawnej poczty elektronicznej.

5. W zakresie bezpiecznej radiowej łączności trankingowej (podsystem SBŁP-T) zapewnia się usługi telekomunikacyjne o minimalnych funkcjonalnościach obejmujących:

1) usługę połączeń głosowych oraz usługę transmisji danych świadczonych z wykorzystaniem szyfrowania komunikacji oraz w sposób zapewniający interoperacyjność z bezpieczną łącznością mobilną;

2) uwierzytelnienie oraz szyfrowaną transmisję głosu i danych oraz odporność transmisji na zakłócenia, a także niezawodność transmisji umożliwiającą dostęp do usług zgodnie z przyjętym scenariuszem operacyjnym.

6. W zakresie bezpiecznej łączności satelitarnej, w tym niejawnej (podsystem SBŁP-S), zapewnia się usługi telekomunikacyjne, które mogą być świadczone z wykorzystaniem dedykowanych urządzeń i rozwiązań kryptograficznych, o minimalnych funkcjonalnościach obejmujących:

1) usługę połączeń głosowych;

2) usługę transmisji danych;

3) usługę transmisji audio-wideo;

4) usługę wiadomości tekstowych.

§ 6. 1. Minimalny poziom bezpieczeństwa usług transmisji danych, połączeń głosowych oraz wiadomości tekstowych przekazywanych w SBŁP obejmuje:

1) powołanie przez operatora SBŁP, dla zapewnienia ciągłości realizacji usług w ramach podsystemów SBŁP, Centrum Zarządzania Siecią, zwanego dalej „NOC”, oraz Operacyjnego Centrum Bezpieczeństwa, zwanego dalej „SOC”;

2) możliwość zlecania przez operatora SBŁP organizatorowi podsystemu SBŁP powołania NOC oraz SOC dla zapewnienia ciągłości realizacji usług w ramach podsystemów SBŁP;

3) szacowanie ryzyka naruszenia bezpieczeństwa elementów infrastruktury SBŁP z uwzględnieniem wpływu czynników zewnętrznych;

4) opracowanie procedury obsługi użytkownika instytucjonalnego;

5) opracowanie procedury reagowania na incydenty oraz wdrożenie zaawansowanych systemów wykrywania i reagowania na incydenty;

6) fizyczne lub logiczne wydzielenie infrastruktury SBŁP lub poszczególnych elementów podsystemów SBŁP;

7) zapewnienie odpowiedniej kontroli dostępu do podsystemów SBŁP wraz z uwierzytelnieniem użytkowników urządzeń końcowych SBŁP;

8) zastosowanie rozwiązań kryptograficznych w celu ochrony danych użytkowników instytucjonalnych przetwarzanych z użyciem rozwiązań chmurowych;

9) pełną redundancję elementów kluczowych dla działania podsystemu SBŁP w zakresie wykorzystywanego sprzętu i oprogramowania, z uwzględnieniem wymogu rozproszenia elementów kluczowych;

10) dywersyfikację przyjętych rozwiązań organizacyjnych i technicznych mających na celu zabezpieczenie przed uzależnieniem świadczenia usług SBŁP od jednego dostawcy lub producenta sprzętu;

11) testy penetracyjne oraz testy interoperacyjności;

12) wdrożenie systemu szkolenia i podnoszenia kwalifikacji kadr.

2. W uzasadnionych przypadkach, związanych z zakresem działania i funkcją podsystemu SBŁP, organizator podsystemu za zgodą operatora SBŁP, może, bez uszczerbku dla bezpieczeństwa tego podsystemu SBŁP oraz zgodnie z wynikiem szacowania ryzyka wobec określonego podsystemu SBŁP, zastosować inne rozwiązania niż określone w ust. 1.

3. Organizator podsystemu, w porozumieniu z operatorem SBŁP, mając na celu utrzymanie minimalnych poziomów dostępności usług SBŁP, zapewnia odpowiednią liczbę wyposażonych zespołów, zdolnych do instalacji, wymiany i usuwania awarii urządzeń, kabli światłowodowych i pozostałej infrastruktury SBŁP.

§ 7. Do zadań NOC należy:

1) reagowanie, rejestrowanie, analiza i klasyfikacja zdarzeń w obszarze usług SBŁP oraz infrastruktury SBŁP;

2) koordynacja usuwania awarii infrastruktury SBŁP;

3) monitoring sieci wchodzących w skład infrastruktury SBŁP, w tym ciągła analiza parametrów sieci, wykrywanie anomalii w ruchu sieciowym, monitorowanie pojemności sieci, analiza trendów i wzorców ruchu oraz wykrywanie potencjalnych zagrożeń;

4) wsparcie techniczne przy usuwaniu awarii związanych z konfiguracją urządzeń wchodzących w skład infrastruktury SBŁP.

§ 8. Do zadań SOC należy:

1) monitorowanie cyberzagrożeń dla podsystemów SBŁP;

2) przeprowadzanie wstępnej analizy alarmów, eliminacja fałszywych alarmów oraz pozyskiwanie danych niezbędnych do obsługi incydentu;

3) obsługa incydentów w ramach zdefiniowanych scenariuszy reakcji oraz przygotowanie rekomendacji i zaleceń dotyczących obsługi incydentów;

4) przygotowywanie raportów dla operatora SBŁP obejmujących zestawienie obsługiwanych incydentów wraz z zaleceniami zmian w infrastrukturze SBŁP, regułach detekcyjnych i scenariuszach reakcji;

5) prowadzenie zaawansowanej diagnostyki incydentów.

§ 9. Rozporządzenie wchodzi w życie z dniem 24 grudnia 2025 r.

Prezes Rady Ministrów: *D. Tusk*