Warszawa, dnia 14 września 2015 r.
Poz. 261

Służba Kontrwywiadu Wojskowego

DECYZJA Nr 364/MON
MINISTRA OBRONY NARODOWEJ

z dnia 10 września 2015 r.

w sprawie wdrożenia i eksploatacji systemu teleinformatycznego ORCHIDEA służącego do realizacji połączeń w trybie niejawnym do klauzuli TAJNE włącznie

Na podstawie art. 2 pkt 1 ustawy z dnia 14 grudnia 1995 r. o urzędzie Ministra Obrony Narodowej (Dz. U. z 2013 r. poz. 189 i 852 oraz z 2014 r. poz. 932) ustala się, co następuje:

1. Uruchamia się w resorcie obrony narodowej system teleinformatyczny ORCHIDEA przeznaczony do przetwarzania informacji niejawnych do klauzuli TAJNE włącznie, zwany dalej „Systemem”.
2. Celem budowanego Systemu jest realizacja utajnionych rozmów telefonicznych i transmisji danych niejawnych pomiędzy komórkami organizacyjnymi i jednostkami organizacyjnymi resortu obrony narodowej poprzez publiczne i resortowe sieci Integrated Services Digital Network, zwane dalej „ISDN”.
3. Kierownikiem jednostki organizującej System jest Szef Służby Kontrwywiadu Wojskowego, zwany dalej „Organizatorem”.
4. Uruchomienie elementów Systemu w danej lokalizacji może nastąpić za zgodą Organizatora na wniosek kierownika komórki organizacyjnej lub jednostki organizacyjnej resortu obrony narodowej – przyszłego użytkownika.
5. Organizator zobowiązany jest do:
   1) koordynacji działań związanych z planowaniem, eksploatacją i wycofaniem Systemu;
   2) opracowania ogólnosystemowej dokumentacji bezpieczeństwa teleinformatycznego;
   3) zapewnienia dokumentów kryptograficznych na potrzeby funkcjonowania Systemu;

4) wyznaczenia osób funkcyjnych Systemu:
   a) głównego administratora Systemu,
   b) głównego inspektora bezpieczeństwa teleinformatycznego,
   c) pełnomocnika ochrony informacji niejawnych w ramach obowiązków wynikających z ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. Nr 182 poz. 1228 oraz z 2015 r. poz. 21),
   d) Oficera Bezpieczeństwa Systemów Łączności i Informatyki;
5) zaopatrzenia jednostek organizacyjnych Służby Kontrwywiadu Wojskowego oraz Narodowego Centrum Kryptologii w dokumenty kryptograficzne;
6) wnioskowania o akredytację bezpieczeństwa teleinformatycznego dla jednostek organizacyjnych Służby Kontrwywiadu Wojskowego.

6. Dyrektor Narodowego Centrum Kryptologii w odniesieniu do komórek organizacyjnych lub jednostek organizacyjnych resortu obrony narodowej:
   1) koordynuje opracowanie i odpowiada za dostarczenie do Organizatora załączników do dokumentacji ogólnosystemowej dla poszczególnych lokalizacji elementów Systemu;
   2) koordynuje proces przydziału terminali ISDN RUMIANEK BRI;
   3) odpowiada za zarządzanie i nadzór nad materiałami kryptograficznymi Systemu;
   4) odpowiada za wsparcie techniczne systemu reagowania na incydenty komputerowe resortu obrony narodowej zgodnie z decyzją Nr 275/MON Ministra Obrony Narodowej z dnia 13 lipca 2015 r. w sprawie organizacji i funkcjonowania systemu reagowania na incydenty komputerowe w resorcie obrony narodowej (Dz. Urz. Min. Obr. Nar. poz. 208);
   5) odpowiada za dystrybucję dokumentów kryptograficznych do urządzeń Systemu.
7. Szef Inspektoratu Systemów Informacyjnych odpowiada za zapewnienie łącz ISDN w ramach posiadanych możliwości technicznych dla wszystkich podmiotów z resortu obrony narodowej, w których planowane będzie uruchomienie Systemu.
8. Kierownicy komórek organizacyjnych lub jednostek organizacyjnych resortu obrony narodowej:
   1) wnioskują do Organizatora o wyrażenie zgody na dołączenie do Systemu nowej lokalizacji;
   2) wyznaczają osoby funkcyjne Systemu będące personelem bezpieczeństwa Systemu zgodnie z opisem w dokumentacji bezpieczeństwa:
      a) lokalnego administratora Systemu,
      b) lokalnego inspektora bezpieczeństwa teleinformatycznego,

c) pełnomocnika ochrony informacji niejawnych w ramach obowiązków wynikających z ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych,

d) Oficera Bezpieczeństwa Systemów Łączności i Informatyki;

3) odpowiadają za opracowanie załączników do dokumentacji ogólnosystemowej w poszczególnych lokalizacjach i przesłanie ich do Dyrektora Narodowego Centrum Kryptologii;

4) akceptują wyniki procesu szacowania ryzyka dla bezpieczeństwa informacji niejawnych i właściwej organizacji bezpieczeństwa teleinformatycznego;

5) wnioskują o akredytację bezpieczeństwa teleinformatycznego;

6) zapewniają bezpieczeństwo eksploatowanym elementom Systemu.

9. Decyzja wchodzi w życie po upływie 14 dni od dnia ogłoszenia.

Minister Obrony Narodowej: *T. Siemoniak*