

Dz.U. 1999 Nr 18 poz. 162

ROZPORZĄDZENIE PREZESA RADY MINISTRÓW

z dnia 25 lutego 1999 r.

w sprawie podstawowych wymagań bezpieczeństwa systemów i sieci teleinformatycznych.

Na podstawie art. 60 ust. 4 ustawy z dnia 22 stycznia 1999 r. o ochronie informacji niejawnych (Dz.U. Nr 11, poz. 95) zarządza się, co następuje:

§ 1.

1. Rozporządzenie określa podstawowe wymagania bezpieczeństwa systemów i sieci teleinformatycznych, zwanego dalej „bezpieczeństwem teleinformatycznym”, w zakresie ochrony fizycznej, elektromagnetycznej i kryptograficznej oraz bezpieczeństwa transmisji, w sieciach lub systemach teleinformatycznych służących do wytwarzania, przetwarzania, przechowywania lub przekazywania informacji niejawnych, a także wytyczne do opracowania szczególnych wymagań bezpieczeństwa tych systemów i sieci.

§ 2.

1. Ilekroć w rozporządzeniu jest mowa o:
 - 1) ustawie - rozumie się przez to ustawę z dnia 22 stycznia 1999 r. o ochronie informacji niejawnych (Dz.U. Nr 11, poz. 95),
 - 2) przetwarzaniu informacji niejawnych – należy przez to rozumieć wytwarzanie, przetwarzanie, przechowywanie lub przekazywanie informacji niejawnych,
 - 3) uwierzytelnieniu – należy przez to rozumieć usługę (funkcję) kryptograficzną pozwalającą sprawdzić i potwierdzić autentyczność wymienianych informacji lub podmiotów uczestniczących w wymianie,
 - 4) algorytmach kryptograficznych – należy przez to rozumieć metodę działania, przekształcającą dane w celu ukrycia lub ujawnienia ich zawartości informacyjnej,
 - 5) kluczach kryptograficznych – należy przez to rozumieć ciąg symboli, od którego w sposób istotny zależy wynik działania algorytmu kryptograficznego.
2. Bezpieczeństwo teleinformatyczne zapewnia się przez:
 - 1) ochronę fizyczną,
 - 2) ochronę elektromagnetyczną,
 - 3) ochronę kryptograficzną,
 - 4) bezpieczeństwo transmisji,
 - 5) kontrole dostępu do urządzeń systemu lub sieci teleinformatycznej.

§ 3.

Kierownik jednostki organizacyjnej jest obowiązany zapewnić bezpieczeństwo teleinformatyczne przed przystąpieniem do przetwarzania informacji niejawnych w systemie lub sieci teleinformatycznej.

§ 4.

Służby ochrony państwa mogą dopuścić do stosowania w systemie lub sieci teleinformatycznej, bez konieczności przeprowadzania badań, urządzenie, które spełnia wymagania bezpieczeństwa określone w rozporządzeniu, jeżeli otrzymało certyfikat właściwej krajowej władzy bezpieczeństwa w państwie będącym stroną Organizacji Traktatu Północnoatlantyckiego.

§ 5.

Ochronę fizyczną systemu lub sieci teleinformatycznej zapewnia się przez:

- 1) umieszczenie urządzeń systemu lub sieci teleinformatycznej w strefach bezpieczeństwa w zależności od:
 - a) klauzuli tajności informacji niejawnych,
 - b) ilości informacji niejawnych,
 - c) zagrożeń w zakresie ujawnienia, utraty, modyfikacji przez osobę nieuprawnioną,
- 2) instalację środków zabezpieczających pomieszczenia, w których znajdują się urządzenia systemu lub sieci teleinformatycznej, w szczególności przed:
 - a) nieuprawnionym dostępem,
 - b) podglądem,
 - c) podsłuchem.

§ 6.

Przetwarzanie informacji niejawnych, stanowiących tajemnicę państwową lub stanowiących tajemnicę służbową, oznaczonych klauzulą „poufne”, w urządzeniach systemu lub sieci teleinformatycznych odbywa się w strefach bezpieczeństwa.

§ 7.

Ochronę elektromagnetyczną systemu lub sieci teleinformatycznej zapewnia się przez umieszczenie urządzeń, połączeń i linii w strefach bezpieczeństwa gwarantujących spełnienie wymogów zabezpieczenia elektromagnetycznego lub zastosowanie urządzeń, połączeń i linii o obniżonym poziomie emisji lub ich ekranowanie i filtrowanie zewnętrznych linii zasilających i sygnałowych.

§ 8.

1. Ochrona kryptograficzna systemu lub sieci teleinformatycznej polega na stosowaniu metod i środków zabezpieczających informacje niejawne stanowiące tajemnicę państwową przez ich szyfrowanie oraz stosowanie innych mechanizmów kryptograficznych gwarantujących integralność i zabezpieczenie przed nieuprawnionym ujawnieniem tych informacji lub uwierzytelnienie podmiotów, lub uwierzytelnienie informacji.
2. Ochronę kryptograficzną systemu lub sieci teleinformatycznej stosuje się przy przekazywaniu w formie elektronicznej informacji, o których mowa w ust. 1, poza strefy bezpieczeństwa.

§ 9.

1. Przemieszczanie urządzeń teleinformatycznych, w których pamięci są informacje niejawne stanowiące tajemnicę państwową lub służbową oznaczone klauzulą „poufne”,

poza strefy bezpieczeństwa wymaga stosowania kryptograficznych metod i środków ochrony tych informacji lub innych środków ochrony, gwarantujących ich zabezpieczenie przed nieuprawnionym ujawnieniem.

2. Przepis ust. 1 stosuje się do elektronicznych nośników danych zawierających informacje niejawne, stanowiące tajemnicę państwową lub służbową oznaczone klauzulą „poufne”, przeznaczonych poza strefę bezpieczeństwa.

§ 10.

1. Do kryptograficznej ochrony informacji niejawnych stanowiących tajemnicę państwową stosuje się, odpowiednio dla klauzuli „tajne” i „ściśle tajne”, algorytmy kryptograficzne oraz środki gwarantujące ochronę tych algorytmów, kluczy kryptograficznych oraz innych istotnych parametrów zabezpieczenia, a w szczególności haseł dostępu.
2. Właściwymi do potwierdzenia przydatności algorytmów i środków, o których mowa w ust. 1, w celu ochrony informacji niejawnych o określonej klauzuli tajności, są służby ochrony państwa.

§ 11.

1. Podłączenie urządzenia systemu lub sieci teleinformatycznej, w których są przetwarzane informacje niejawne stanowiące tajemnicę państwową, do powszechnie dostępnego urządzenia systemu lub sieci jest dopuszczalne pod warunkiem zastosowania metod i środków, o których mowa w § 8.
2. Podłączenie urządzenia systemu lub sieci teleinformatycznej, w którym są przetwarzane informacje niejawne stanowiące tajemnicę służbową, do powszechnie dostępnego urządzenia systemu lub sieci jest dopuszczalne pod warunkiem zastosowania właściwych mechanizmów kontroli dostępu, o których mowa w § 12 ust. 2.

§ 12.

1. W celu zapewnienia kontroli dostępu do systemu lub sieci teleinformatycznej:
 - 1) kierownik jednostki organizacyjnej określa warunki i sposób przydzielania uprawnień ich użytkownikom,
 - 2) administrator systemów i sieci teleinformatycznych określa warunki oraz sposób przydzielania tym użytkownikom kont i haseł, a także zapewnia właściwe wykorzystanie mechanizmów, o których mowa w ust. 2.
2. System lub sieć teleinformatyczną wyposaża się w mechanizmy kontroli dostępu odpowiednie do klauzuli tajności informacji niejawnych przetwarzanych w tych systemach lub sieciach.

§ 13.

System lub sieć teleinformatyczna, w której są przetwarzane informacje niejawne stanowiące tajemnicę państwową, projektuje się, organizuje i eksploatuje w sposób uniemożliwiający niekontrolowany dostęp jednej osoby do wszystkich zasobów systemu lub sieci, w szczególności do danych, oprogramowania i urządzeń.

§ 14.

1. Szczególne wymagania bezpieczeństwa opracowuje się, po dokonaniu analizy przewidywanych zagrożeń, indywidualnie dla każdego systemu lub sieci teleinformatycznej, w której mają być przetwarzane informacje niejawne, z uwzględnieniem warunków charakterystycznych dla jednostki organizacyjnej.

2. Szczególne wymagania bezpieczeństwa formułuje się na etapie projektowania nowego systemu lub sieci teleinformatycznej, a następnie uzupełnia i rozwija wraz z wdrażaniem, eksploatacją i modernizacją tego systemu lub sieci.

§ 15.

Szczególne wymagania bezpieczeństwa systemu lub sieci teleinformatycznych powinny określać wielkość i lokalizację stref bezpieczeństwa oraz środki ich ochrony odpowiednie dla danej jednostki organizacyjnej.

§ 16.

Przy opracowaniu szczególnych wymagań bezpieczeństwa należy uwzględnić:

- 1) charakterystykę systemu lub sieci teleinformatycznych,
- 2) dane o budowie systemu lub sieci teleinformatycznej,
- 3) określenie środków ochrony zapewniających bezpieczeństwo informacji niejawnych, przetwarzanych w systemie lub sieci teleinformatycznej, przed możliwością narażenia ich bezpieczeństwa, a w szczególności nieuprawnionym ujawnieniem,
- 4) zadania administratora systemu lub sieci teleinformatycznej i pracownika pionu, o których mowa w art. 63 ust. 1 ustawy.

§ 17.

Charakterystyka systemu lub sieci teleinformatycznej powinna określać:

- 1) klauzulę tajności informacji niejawnych, które będą przetwarzane w systemie lub sieci teleinformatycznej,
- 2) kategorie uprawnień użytkowników systemu lub sieci teleinformatycznej w zakresie dostępu do przetwarzanych w nich informacji niejawnych, w zależności od klauzuli tajności tych informacji.

§ 18.

Dane o budowie systemu lub sieci teleinformatycznej zawierają informacje dotyczące tego systemu lub sieci w zakresie:

- 1) lokalizacji,
- 2) typu wykorzystywanych w nich urządzeń oraz oprogramowania,
- 3) sposobu realizowania połączeń wewnętrznych oraz zewnętrznych,
- 4) konfiguracji sprzętowej,
- 5) środowiska eksploatacji.

§ 19.

Środki ochrony, o których mowa w § 16 pkt. 3, powinny uwzględniać wskazanie osób odpowiedzialnych za bezpieczeństwo systemu lub sieci teleinformatycznej oraz określać procedury bezpieczeństwa związane z jego eksploatacją i kontrolą, a także wskazywać szczegółowe wymagania w zakresie szkoleń dla administratorów, pracowników pionu i wszystkich użytkowników systemu lub sieci.

§ 20.

Rozporządzenie wchodzi w życie z dniem 11 marca 1999 r.

