1433

ROZPORZĄDZENIE PREZESA RADY MINISTRÓW

z dnia 25 sierpnia 2005 r.

w sprawie podstawowych wymagań bezpieczeństwa teleinformatycznego

Na podstawie art. 62 ust. 1 ustawy z dnia 22 stycznia 1999 r. o ochronie informacji niejawnych (Dz. U. Nr 11, poz. 95, z późn. zm.[1)]) zarządza się, co następuje:

Rozdział 1

Przepisy ogólne

§ 1. Rozporządzenie określa:

1) podstawowe wymagania bezpieczeństwa teleinformatycznego, jakim powinny odpowiadać systemy i sieci teleinformatyczne służące do wytwarzania, przetwarzania, przechowywania lub przekazywania informacji niejawnych;

2) sposób opracowywania dokumentów szczególnych wymagań bezpieczeństwa i procedur bezpiecznej eksploatacji systemów lub sieci teleinformatycznych.

§ 2. Ilekroć w rozporządzeniu jest mowa o:

1) incydencie bezpieczeństwa teleinformatycznego — należy przez to rozumieć każde zdarzenie naruszające bezpieczeństwo teleinformatyczne spowodowane w szczególności awarią systemu lub sieci teleinformatycznej, działaniem osób uprawnionych lub nieuprawnionych do pracy w tym systemie lub sieci albo zaniechaniem osób uprawnionych;

2) przekazywaniu informacji niejawnych — należy przez to rozumieć zarówno transmisję informacji niejawnych, jak i przekazywanie elektronicznego nośnika danych, na którym zostały one utrwalone;

3) przetwarzaniu informacji niejawnych — należy przez to rozumieć także wytwarzanie, przechowywanie lub przekazywanie informacji niejawnych.

Rozdział 2

Podstawowe wymagania bezpieczeństwa teleinformatycznego

§ 3. 1. Bezpieczeństwo teleinformatyczne zapewnia się, chroniąc informacje przetwarzane w systemach i sieciach teleinformatycznych przed utratą właściwości gwarantujących to bezpieczeństwo, w szczególności przed utratą poufności, dostępności i integralności.

2. Bezpieczeństwo teleinformatyczne zapewnia się przed rozpoczęciem oraz w trakcie przetwarzania informacji niejawnych w systemie lub sieci teleinformatycznej.

§ 4. Za właściwą organizację bezpieczeństwa teleinformatycznego odpowiada kierownik jednostki organizacyjnej, który w szczególności:

1) zapewnia opracowanie dokumentacji bezpieczeństwa teleinformatycznego;
2) realizuje ochronę fizyczną, elektromagnetyczną i kryptograficzną systemu lub sieci teleinformatycznej;
3) zapewnia niezawodność transmisji oraz kontrolę dostępu do urządzeń systemu lub sieci teleinformatycznej;
4) dokonuje analizy stanu bezpieczeństwa teleinformatycznego oraz zapewnia usunięcie stwierdzonych nieprawidłowości;
5) zapewnia przeszkolenie z zakresu bezpieczeństwa teleinformatycznego dla osób uprawnionych do pracy w systemie lub sieci teleinformatycznej;
6) zawiadamia właściwą służbę ochrony państwa o zaistniałym incydencie bezpieczeństwa teleinformatycznego dotyczącym informacji niejawnych oznaczonych co najmniej klauzulą „poufne".

§ 5. Ochrona fizyczna systemu lub sieci teleinformatycznej polega na:

1) umieszczeniu urządzeń systemu lub sieci teleinformatycznej w strefie bezpieczeństwa, strefie administracyjnej lub specjalnej strefie bezpieczeństwa, zwanych dalej „strefą kontrolowanego dostępu" w zależności od:
   a) klauzuli tajności,
   b) ilości,
   c) zagrożeń dla poufności, integralności lub dostępności
   — informacji niejawnych;
2) zastosowaniu środków zapewniających ochronę fizyczną, w szczególności przed:
   a) nieuprawnionym dostępem,
   b) podglądem,
   c) podsłuchem.

§ 6. 1. Ochrona elektromagnetyczna systemu lub sieci teleinformatycznej polega na niedopuszczeniu do utraty poufności i dostępności informacji niejawnych przetwarzanych w urządzeniach teleinformatycznych.

[1)] Zmiany wymienionej ustawy zostały ogłoszone w Dz. U. z 2000 r. Nr 12, poz. 136 i Nr 39, poz. 462, z 2001 r. Nr 22, poz. 247, Nr 27, poz. 298, Nr 56, poz. 580, Nr 110, poz. 1189, Nr 123, poz. 1353 i Nr 154, poz. 1800, z 2002 r. Nr 74, poz. 676, Nr 89, poz. 804 i Nr 153, poz. 1271, z 2003 r. Nr 17, poz. 155, z 2004 r. Nr 29, poz. 257 oraz z 2005 r. Nr 85, poz. 727.

2. Utrata poufności następuje w szczególności na skutek wykorzystania elektromagnetycznej emisji ujawniającej pochodzącej z tych urządzeń.

3. Utrata dostępności następuje w szczególności na skutek zakłócania pracy urządzeń teleinformatycznych za pomocą impulsów elektromagnetycznych o dużej mocy.

4. Ochronę elektromagnetyczną systemu lub sieci teleinformatycznej zapewnia się w szczególności przez umieszczenie urządzeń teleinformatycznych, połączeń i linii w strefach kontrolowanego dostępu spełniających wymagania w zakresie tłumienności elektromagnetycznej odpowiednio do wyników szacowania ryzyka dla informacji niejawnych, o którym mowa w § 12, lub zastosowanie odpowiednich urządzeń teleinformatycznych, połączeń i linii o obniżonym poziomie emisji lub ich ekranowanie z jednoczesnym filtrowaniem zewnętrznych linii zasilających i sygnałowych.

§ 7. 1. Ochrona kryptograficzna informacji niejawnych przetwarzanych w systemie lub sieci teleinformatycznej polega na zastosowaniu mechanizmów gwarantujących ich poufność, integralność oraz uwierzytelnienie.

2. Ochronę kryptograficzną stosuje się przy przekazywaniu informacji niejawnych w formie transmisji poza strefę kontrolowanego dostępu.

3. Przekazywanie informacji niejawnych utrwalonych na elektronicznych nośnikach danych poza strefę kontrolowanego dostępu odbywa się z zapewnieniem, odpowiedniej do klauzuli tajności tych informacji, ochrony kryptograficznej lub po spełnieniu wymagań, o których mowa w przepisach w sprawie trybu i sposobu przyjmowania, przewożenia, wydawania i ochrony materiałów, w celu ich zabezpieczenia przed nieuprawnionym ujawnieniem, utratą, uszkodzeniem lub zniszczeniem.

§ 8. Niezawodność transmisji polega na zapewnieniu integralności i dostępności informacji niejawnych przekazywanych w systemach lub sieciach teleinformatycznych. Zapewnia się ją w szczególności przez wykorzystywanie zapasowych łączy telekomunikacyjnych.

§ 9. 1. W celu zapewnienia kontroli dostępu do systemu lub sieci teleinformatycznej:

1) kierownik jednostki organizacyjnej lub osoba przez niego upoważniona ustala warunki i sposób przydzielania uprawnień osobom uprawnionym do pracy w systemie lub sieci teleinformatycznej;

2) administrator systemów określa warunki oraz sposób przydzielania tym osobom kont oraz mechanizmów kontroli dostępu, a także zapewnia ich właściwe wykorzystanie.

2. System lub sieć teleinformatyczną wyposaża się w mechanizmy kontroli dostępu odpowiednie do klauzuli tajności informacji niejawnych w nich przetwarzanych.

§ 10. Projektowanie, organizacja i eksploatacja systemu lub sieci teleinformatycznej służącej do przetwarzania informacji niejawnych stanowiących tajemnicę państwową odbywa się w sposób uniemożliwiający niekontrolowany dostęp jednej osoby do wszystkich zasobów systemu lub sieci, w szczególności danych, informacji, oprogramowania, narzędzi lub urządzeń teleinformatycznych.

§ 11. Służby ochrony państwa mogą dopuścić do stosowania w systemie lub sieci teleinformatycznej urządzenia lub narzędzia, które spełniają właściwe wymagania bezpieczeństwa, jeżeli otrzymały stosowny certyfikat krajowej władzy bezpieczeństwa w państwie będącym stroną Organizacji Traktatu Północnoatlantyckiego lub w państwie członkowskim Unii Europejskiej.

Rozdział 3

Sposób opracowywania dokumentacji bezpieczeństwa teleinformatycznego

§ 12. Dokumenty szczególnych wymagań bezpieczeństwa opracowuje się po przeprowadzeniu szacowania ryzyka dla informacji niejawnych, które mają być przetwarzane w danym systemie lub sieci teleinformatycznej, z uwzględnieniem warunków charakterystycznych dla jednostki organizacyjnej.

§ 13. 1. Przy opracowaniu szczególnych wymagań bezpieczeństwa systemu lub sieci teleinformatycznej uwzględnia się w szczególności dane o budowie oraz charakterystykę systemu lub sieci teleinformatycznej.

2. Dane o budowie systemu lub sieci teleinformatycznej obejmują dane dotyczące elementów wchodzących w skład tego systemu lub sieci w zakresie:

1) lokalizacji;

2) typu wykorzystywanych urządzeń oraz oprogramowania;

3) sposobu realizowania połączeń wewnętrznych oraz zewnętrznych;

4) konfiguracji sprzętowej i ustawień mechanizmów zabezpieczających;

5) środowiska eksploatacji.

3. Charakterystyka systemu lub sieci teleinformatycznej powinna określać:

1) klauzulę tajności informacji niejawnych, które będą w nich przetwarzane;

2) kategorie uprawnień osób uprawnionych do pracy w systemie lub sieci teleinformatycznej w zakresie dostępu do przetwarzanych w nich informacji niejawnych, w zależności od klauzuli tajności tych informacji;

3) tryb bezpieczeństwa pracy systemu lub sieci teleinformatycznej.

§ 14. Szczególne wymagania bezpieczeństwa określają co najmniej:

1) osoby odpowiedzialne za wdrożenie środków zapewniających bezpieczeństwo teleinformatyczne;

2) zadania osób odpowiedzialnych za bezpieczeństwo teleinformatyczne;

3) granice i lokalizację stref kontrolowanego dostępu oraz środki ich ochrony;

4) środki ochrony kryptograficznej, elektromagnetycznej, technicznej lub organizacyjnej systemu lub sieci teleinformatycznej;

5) inne zastosowane środki ochrony zapewniające bezpieczeństwo teleinformatyczne informacji niejawnych;

6) zasady zarządzania ryzykiem;

7) zasady szkolenia z zakresu bezpieczeństwa teleinformatycznego osób odpowiedzialnych za bezpieczeństwo teleinformatyczne oraz osób uprawnionych do pracy w systemie lub sieci teleinformatycznej.

§ 15. 1. Procedury bezpiecznej eksploatacji zawierają szczegółowy wykaz czynności wraz z dokładnym opisem sposobu ich wykonania, które powinny być realizowane przez osoby odpowiedzialne za bezpieczeństwo teleinformatyczne oraz osoby uprawnione do pracy w systemie lub sieci teleinformatycznej.

2. Szczegółowy wykaz czynności powinien być ujęty w tematycznie wyodrębnione procedury bezpieczeństwa dotyczące w szczególności:

1) administrowania systemem lub siecią teleinformatyczną;

2) bezpieczeństwa osobowego;

3) bezpieczeństwa dokumentów i materiałów niejawnych, w tym procedur sporządzania kopii z tych dokumentów oraz niszczenia dokumentów i ich kopii;

4) ochrony kryptograficznej, elektromagnetycznej, fizycznej, niezawodności transmisji lub kontroli dostępu do urządzeń systemu lub sieci teleinformatycznej;

5) bezpieczeństwa urządzeń i oprogramowania;

6) zapewnienia ciągłości działania systemu lub sieci teleinformatycznej;

7) zarządzania konfiguracją;

8) audytu bezpieczeństwa.

§ 16. W procedurach, o których mowa w § 15, określa się tryb postępowania przez osoby odpowiedzialne za bezpieczeństwo teleinformatyczne oraz osoby uprawnione do pracy w systemie lub sieci teleinformatycznej w sytuacji wystąpienia incydentu bezpieczeństwa teleinformatycznego.

Rozdział 4

Przepisy końcowe

§ 17. Traci moc rozporządzenie Prezesa Rady Ministrów z dnia 25 lutego 1999 r. w sprawie podstawowych wymagań bezpieczeństwa systemów i sieci teleinformatycznych (Dz. U. Nr 18, poz. 162).

§ 18. Rozporządzenie wchodzi w życie po upływie 14 dni od dnia ogłoszenia.

Prezes Rady Ministrów: *M. Belka*