948

ROZPORZĄDZENIE PREZESA RADY MINISTRÓW

z dnia 20 lipca 2011 r.

w sprawie podstawowych wymagań bezpieczeństwa teleinformatycznego

Na podstawie art. 49 ust. 9 ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. Nr 182, poz. 1228) zarządza się, co następuje:

Rozdział 1

Przepisy ogólne

§ 1. Rozporządzenie określa:

1) podstawowe wymagania bezpieczeństwa teleinformatycznego, jakim powinny odpowiadać systemy teleinformatyczne, o których mowa w art. 48 ust. 1 ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych, zwanej dalej „ustawą”;

2) niezbędne dane, jakie powinna zawierać dokumentacja bezpieczeństwa systemów teleinformatycznych oraz sposób jej opracowywania.

§ 2. Ilekroć w rozporządzeniu jest mowa o:

1) dostępności — należy przez to rozumieć właściwość określającą, że zasób systemu teleinformatycznego jest możliwy do wykorzystania na żądanie, w określonym czasie, przez podmiot uprawniony do pracy w systemie teleinformatycznym;

2) elektromagnetycznej emisji ujawniającej — należy przez to rozumieć sygnały elektromagnetyczne związane z przetwarzaniem informacji w systemach teleinformatycznych, powstające w sposób naturalny, ale niezamierzony, które odebrane i poddane analizie mogą prowadzić do odtworzenia fragmentu lub całości przetwarzanej informacji niejawnej;

3) incydencie bezpieczeństwa teleinformatycznego — należy przez to rozumieć takie pojedyncze zdarzenie lub serię zdarzeń, związanych z bezpieczeństwem informacji niejawnych, które zagrażają ich poufności, dostępności lub integralności;

4) informatycznym nośniku danych — należy przez to rozumieć materiał służący do zapisywania, przechowywania i odczytywania danych w postaci cyfrowej;

5) integralności — należy przez to rozumieć właściwość określającą, że zasób systemu teleinformatycznego nie został zmodyfikowany w sposób nieuprawniony;

6) oprogramowaniu złośliwym — należy przez to rozumieć oprogramowanie, którego celem jest przeprowadzenie nieuprawnionych lub szkodliwych działań w systemie teleinformatycznym;

7) podatności — należy przez to rozumieć słabość zasobu lub zabezpieczenia systemu teleinformatycznego, która może zostać wykorzystana przez zagrożenie;

8) połączeniu międzysystemowym — należy przez to rozumieć techniczne lub organizacyjne połączenie dwóch lub więcej systemów teleinformatycznych, umożliwiające ich współpracę, a w szczególności wymianę danych;

9) poufności — należy przez to rozumieć właściwość określającą, że informacja nie jest ujawniana podmiotom do tego nieuprawnionym;

10) przekazywaniu informacji — należy przez to rozumieć zarówno transmisję informacji, jak i przekazywanie informacji na informatycznych nośnikach danych, na których zostały utrwalone;

11) testach bezpieczeństwa — należy przez to rozumieć testy poprawności i skuteczności funkcjonowania zabezpieczeń w systemie teleinformatycznym;

12) zabezpieczeniu — należy przez to rozumieć środki o charakterze fizycznym, technicznym lub organizacyjnym zmniejszające ryzyko;

13) zagrożeniu — należy przez to rozumieć potencjalną przyczynę niepożądanego zdarzenia, które może wywołać szkodę w zasobach systemu teleinformatycznego;

14) zaleceniach — należy przez to rozumieć zalecenia w zakresie bezpieczeństwa teleinformatycznego, o których mowa w art. 52 ust. 3 ustawy;

15) zasobach systemu teleinformatycznego — należy przez to rozumieć informacje przetwarzane w systemie teleinformatycznym, jak również osoby, usługi, oprogramowanie, dane i sprzęt oraz inne elementy mające wpływ na bezpieczeństwo tych informacji.

§ 3. Ze względu na posiadane przez użytkowników systemu teleinformatycznego uprawnienia dostępu do informacji niejawnych system teleinformatyczny przeznaczony do przetwarzania informacji niejawnych może funkcjonować w jednym z następujących trybów bezpieczeństwa pracy:

1) dedykowanym — w którym spełnione są łącznie następujące warunki:

   a) wszyscy użytkownicy posiadają uprawnienie do dostępu do informacji niejawnych o najwyższej klauzuli tajności, jakie mogą być przetwarzane w tym systemie teleinformatycznym,

   b) wszyscy użytkownicy mają uzasadnioną potrzebę dostępu do wszystkich informacji niejawnych przetwarzanych w systemie teleinformatycznym;

2) systemowym — w którym spełnione są łącznie następujące warunki:

a) wszyscy użytkownicy posiadają uprawnienie do dostępu do informacji niejawnych o najwyższej klauzuli tajności, jakie mogą być przetwarzane w tym systemie teleinformatycznym,

b) nie wszyscy użytkownicy mają uzasadnioną potrzebę dostępu do wszystkich informacji niejawnych przetwarzanych w systemie teleinformatycznym;

3) wielopoziomowym — w którym spełnione są łącznie następujące warunki:

a) nie wszyscy użytkownicy posiadają uprawnienie do dostępu do informacji niejawnych o najwyższej klauzuli tajności, jakie mogą być przetwarzane w tym systemie teleinformatycznym,

b) nie wszyscy użytkownicy mają uzasadnioną potrzebę dostępu do wszystkich informacji niejawnych przetwarzanych w systemie teleinformatycznym.

§ 4. Jednostka organizująca system teleinformatyczny przeznaczony do przetwarzania informacji niejawnych międzynarodowych uwzględnia przy jego organizowaniu wymagania bezpieczeństwa teleinformatycznego wynikające z umów międzynarodowych.

Rozdział 2

Podstawowe wymagania bezpieczeństwa teleinformatycznego

§ 5. 1. Bezpieczeństwo informacji niejawnych przetwarzanych w systemie teleinformatycznym zapewnia się przez wdrożenie spójnego zbioru zabezpieczeń w celu zapewnienia poufności, integralności i dostępności tych informacji.

2. Cel, o którym mowa w ust. 1, osiąga się przez:

1) objęcie systemu teleinformatycznego procesem zarządzania ryzykiem dla bezpieczeństwa informacji niejawnych przetwarzanych w systemie teleinformatycznym, zwanego dalej „zarządzaniem ryzykiem w systemie teleinformatycznym”;

2) ograniczenie zaufania, polegające na traktowaniu innych systemów teleinformatycznych jako potencjalnych źródeł zagrożeń oraz wdrożeniu w systemie teleinformatycznym zabezpieczeń kontrolujących wymianę informacji z tymi systemami teleinformatycznymi;

3) wprowadzenie wielopoziomowej ochrony systemu teleinformatycznego, polegającej na stosowaniu zabezpieczeń na możliwie wielu różnych poziomach organizacji ochrony systemu teleinformatycznego, w celu ograniczenia występowania przypadków, w których przełamanie pojedynczego zabezpieczenia skutkuje naruszeniem celu, o którym mowa w ust. 1;

4) wykonywanie okresowych testów bezpieczeństwa;

5) ograniczanie uprawnień, polegające na nadawaniu użytkownikom systemu teleinformatycznego wyłącznie uprawnień niezbędnych do wykonywania pracy;

6) minimalizację funkcjonalności, polegającą na instalowaniu, uaktywnianiu i wykorzystywaniu w systemie teleinformatycznym wyłącznie funkcji, protokołów komunikacyjnych i usług niezbędnych do prawidłowej realizacji zadań, do których system teleinformatyczny został przeznaczony.

§ 6. W celu zapewnienia ochrony przed nieuprawnionym dostępem do systemu teleinformatycznego:

1) ustala się warunki i sposób przydzielania użytkownikom uprawnień do pracy w systemie teleinformatycznym;

2) chroni się informacje i materiały umożliwiające dostęp do systemu teleinformatycznego;

3) chroni się elementy systemu teleinformatycznego istotne dla jego bezpieczeństwa oraz wdraża się je w sposób zapewniający możliwość wykrycia wprowadzenia nieuprawnionych zmian lub prób ich wprowadzenia.

§ 7. Przed dopuszczeniem osób do pracy w systemie teleinformatycznym kierownik jednostki organizacyjnej zapewnia ich przeszkolenie z zakresu bezpieczeństwa teleinformatycznego oraz zapoznanie z procedurami bezpiecznej eksploatacji w zakresie, jaki ich dotyczy.

§ 8. 1. W celu niedopuszczenia do utraty poufności informacji niejawnych na skutek wykorzystania elektromagnetycznej emisji ujawniającej, która pochodzi z elementów systemu, w systemie teleinformatycznym przetwarzającym informacje niejawne o klauzuli „poufne” lub wyższej stosuje się środki ochrony elektromagnetycznej dobierane na podstawie wyników szacowania ryzyka dla bezpieczeństwa informacji niejawnych, z uwzględnieniem zaleceń.

2. W celu niedopuszczenia do utraty dostępności informacji niejawnych przetwarzanych w urządzeniach teleinformatycznych na skutek zakłócania ich pracy za pomocą emisji lub impulsów elektromagnetycznych o dużej mocy stosuje się środki ochrony elektromagnetycznej dobierane na podstawie wyników szacowania ryzyka dla bezpieczeństwa informacji niejawnych.

§ 9. 1. W celu zapewnienia dostępności zasobów w systemie teleinformatycznym ustala się:

1) zasady tworzenia i przechowywania kopii zapasowych;

2) procedury postępowania w sytuacjach kryzysowych, w tym w przypadkach awarii elementów systemu teleinformatycznego;

3) procedury monitorowania stanu technicznego systemu teleinformatycznego.

2. W zależności od potrzeb oraz wyników szacowania ryzyka dla bezpieczeństwa informacji niejawnych, w celu zapewnienia dostępności zasobów systemu teleinformatycznego stosuje się w szczególności alternatywne łącza telekomunikacyjne, alternatywne urządzenia lub zasilanie awaryjne.

§ 10. 1. W zależności od potrzeb oraz wyników szacowania ryzyka dla bezpieczeństwa informacji niejawnych, transmisję danych pomiędzy elementami systemu teleinformatycznego chroni się przed wykryciem, przechwyceniem lub zakłócaniem.

2. Poufność informacji niejawnych przekazywanych w formie transmisji poza strefami ochronnymi zapewnia się przez stosowanie urządzeń lub narzędzi kryptograficznych, certyfikowanych zgodnie z art. 50 ust. 2 ustawy lub dopuszczonych w trybie art. 50 ust. 7 ustawy, odpowiednich do klauzuli tajności przekazywanych informacji.

3. W szczególnie uzasadnionych przypadkach, biorąc pod uwagę wyniki szacowania ryzyka dla bezpieczeństwa informacji niejawnych, środki ochrony kryptograficznej, o których mowa w ust. 2, mogą zostać uzupełnione lub zastąpione zabezpieczeniami innymi niż kryptograficzne.

§ 11. W zakresie niezbędnym do zapewnienia przeglądu, analizy oraz dostarczania dowodów działań naruszających bezpieczeństwo informacji niejawnych, dla systemu teleinformatycznego przetwarzającego informacje niejawne tworzy się i przechowuje rejestry zdarzeń oraz zapewnia się ich poufność, integralność i dostępność.

§ 12. System teleinformatyczny wyposaża się w mechanizmy lub procedury zapobiegające incydentom bezpieczeństwa teleinformatycznego, w tym zabezpieczające przed działaniem oprogramowania złośliwego, a także umożliwiające jak najszybsze wykrywanie incydentów bezpieczeństwa teleinformatycznego oraz zapewniające niezwłoczne informowanie odpowiednich osób o wykrytym incydencie.

§ 13. Administrator systemu teleinformatycznego bierze udział w tworzeniu dokumentacji bezpieczeństwa systemu teleinformatycznego oraz w procesie zarządzania ryzykiem w systemie teleinformatycznym:

1) realizując szkolenia użytkowników systemu teleinformatycznego;

2) utrzymując zgodność systemu teleinformatycznego z jego dokumentacją bezpieczeństwa;

3) wdrażając zabezpieczenia w systemie teleinformatycznym.

§ 14. Inspektor bezpieczeństwa teleinformatycznego bierze udział w procesie zarządzania ryzykiem w systemie teleinformatycznym, weryfikując:

1) poprawność realizacji zadań przez administratora, w tym właściwe zarządzanie konfiguracją oraz uprawnieniami przydzielanymi użytkownikom;

2) znajomość i przestrzeganie przez użytkowników zasad ochrony informacji niejawnych oraz procedur bezpiecznej eksploatacji w systemie teleinformatycznym, w tym w zakresie wykorzystywania urządzeń i narzędzi służących do ochrony informacji niejawnych;

3) stan zabezpieczeń systemu teleinformatycznego, w tym analizując rejestry zdarzeń systemu teleinformatycznego.

§ 15. 1. W przypadku organizacji połączenia międzysystemowego uwzględnia się wymaganie ograniczonego zaufania, o którym mowa w § 5 ust. 2 pkt 2.

2. Organizując połączenie międzysystemowe, wdraża się zabezpieczenia uniemożliwiające przekazywanie niepożądanych informacji pomiędzy łączonymi systemami teleinformatycznymi, w szczególności uniemożliwiające przekazywanie informacji o wyższej klauzuli tajności do systemu teleinformatycznego przetwarzającego informacje o klauzuli niższej.

§ 16. Urządzenie, narzędzie lub środek przeznaczony do ochrony informacji niejawnych, dla którego został wydany przez Agencję Bezpieczeństwa Wewnętrznego, zwaną dalej „ABW”, lub Służbę Kontrwywiadu Wojskowego, zwaną dalej „SKW”, certyfikat, o którym mowa w art. 50 ust. 4 ustawy, podlega ochronie do momentu jego zniszczenia lub wycofania, zgodnie z zaleceniami ABW lub SKW.

§ 17. 1. Informatyczne nośniki danych przeznaczone do przetwarzania informacji niejawnych obejmuje się ochroną od momentu oznaczenia nośnika klauzulą tajności aż do trwałego usunięcia danych na nim zapisanych oraz zniesienia klauzuli tajności albo do momentu jego zniszczenia.

2. Informacje niejawne przekazywane poza strefę ochronną na informatycznych nośnikach danych chroni się:

1) z wykorzystaniem urządzeń lub narzędzi kryptograficznych, certyfikowanych zgodnie z art. 50 ust. 2 ustawy lub dopuszczonych w trybie art. 50 ust. 7 ustawy, odpowiednich do klauzuli tajności przekazywanych informacji, lub

2) przez spełnienie 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.

3. Sposób i metody trwałego usuwania danych oraz niszczenia informatycznych nośników danych określa się z uwzględnieniem zaleceń.

4. Klauzula tajności informatycznych nośników danych umożliwiających wielokrotny zapis, na których zapisano informacje niejawne oznaczone klauzulą „tajne” lub „ściśle tajne”, nie podlega zniesieniu lub obniżeniu.

§ 18. 1. Bezpieczeństwo informacji niejawnych przetwarzanych w systemie teleinformatycznym uwzględnia się w całym cyklu funkcjonowania systemu teleinformatycznego, składającym się z etapów:

1) planowania;

2) projektowania;

3) wdrażania;

4) eksploatacji;

5) wycofywania.

2. Na etapie planowania ustala się potrzeby w zakresie przetwarzania informacji niejawnych w systemie teleinformatycznym, w szczególności określa się:

1) przeznaczenie systemu teleinformatycznego;

2) maksymalną klauzulę tajności informacji niejawnych, które będą przetwarzane w systemie teleinformatycznym;

3) tryb bezpieczeństwa pracy systemu teleinformatycznego;

4) szacunkową liczbę użytkowników;

5) planowaną lokalizację.

3. Na etapie projektowania:

1) przeprowadza się wstępne szacowanie ryzyka dla bezpieczeństwa informacji niejawnych w celu określenia wymagań dla zabezpieczeń;

2) dokonuje się wyboru zabezpieczeń dla systemu teleinformatycznego w oparciu o wyniki wstępnego szacowania ryzyka dla bezpieczeństwa informacji niejawnych;

3) uzgadnia się z podmiotem akredytującym plan akredytacji obejmujący zakres i harmonogram przedsięwzięć wymaganych do uzyskania akredytacji bezpieczeństwa teleinformatycznego;

4) uzgadnia się z podmiotem zaopatrującym w klucze kryptograficzne rodzaj oraz ilość niezbędnych urządzeń lub narzędzi kryptograficznych, a także sposób ich wykorzystania;

5) opracowuje się dokument szczególnych wymagań bezpieczeństwa.

4. Na etapie wdrażania:

1) pozyskuje i wdraża się urządzenia lub narzędzia realizujące zabezpieczenia w systemie teleinformatycznym;

2) przeprowadza się testy bezpieczeństwa systemu teleinformatycznego;

3) przeprowadza się szacowanie ryzyka dla bezpieczeństwa informacji niejawnych z uwzględnieniem wprowadzonych zabezpieczeń;

4) opracowuje się dokument procedur bezpiecznej eksploatacji oraz uzupełnia dokument szczególnych wymagań bezpieczeństwa;

5) system teleinformatyczny poddaje się akredytacji bezpieczeństwa teleinformatycznego.

5. Na etapie eksploatacji:

1) utrzymuje się zgodność systemu teleinformatycznego z jego dokumentacją bezpieczeństwa;

2) zapewnia się ciągłość procesu zarządzania ryzykiem w systemie teleinformatycznym;

3) okresowo przeprowadza się testy bezpieczeństwa w celu weryfikacji poprawności działania poszczególnych zabezpieczeń oraz usuwa stwierdzone nieprawidłowości;

4) w zależności od potrzeb wprowadza się zmiany do systemu teleinformatycznego oraz, jeżeli jest to właściwe, wykonuje testy bezpieczeństwa, a także uaktualnia dokumentację bezpieczeństwa systemu teleinformatycznego, przy czym modyfikacje mogące mieć wpływ na bezpieczeństwo systemu teleinformatycznego wymagają zgody podmiotu, który udzielił akredytacji bezpieczeństwa teleinformatycznego, zaś w przypadku systemów teleinformatycznych, o których mowa w art. 48 ust. 9 i 10 ustawy — przekazania, odpowiednio do ABW albo SKW, w terminie 30 dni od wprowadzenia wyżej wymienionych modyfikacji, uaktualnionej dokumentacji bezpieczeństwa systemu teleinformatycznego, w szczególności w formie aneksów.

6. Na etapie wycofywania:

1) zaprzestaje się eksploatacji systemu teleinformatycznego;

2) powiadamia się pisemnie ABW albo SKW o wycofaniu systemu z eksploatacji;

3) zwraca się do ABW albo SKW świadectwo akredytacji bezpieczeństwa systemu teleinformatycznego, jeżeli system teleinformatyczny przeznaczony był do przetwarzania informacji niejawnych o klauzuli „poufne” lub wyższej;

4) usuwa się informacje niejawne z systemu teleinformatycznego, w szczególności przez przeniesienie ich do innego systemu teleinformatycznego, zarchiwizowanie lub zniszczenie informatycznych nośników danych.

Rozdział 3

Zarządzanie ryzykiem w systemie teleinformatycznym

§ 19. 1. Proces zarządzania ryzykiem w systemie teleinformatycznym prowadzi się w celu zapewnienia i utrzymania na poziomie akceptowanym przez kierownika danej jednostki organizacyjnej bezpieczeństwa informacji niejawnych przetwarzanych w tym systemie.

2. Zarządzanie ryzykiem w systemie teleinformatycznym prowadzi się, realizując procesy:

1) szacowania ryzyka dla bezpieczeństwa informacji niejawnych;

2) postępowania z ryzykiem;

3) akceptacji ryzyka;

4) przeglądu, monitorowania i informowania o ryzyku.

3. Przed przeprowadzeniem procesu szacowania ryzyka:

1) ustala się granice i zakres analizy ryzyka;

2) ustanawia się strukturę organizacyjną odpowiedzialną za zarządzanie ryzykiem w systemie teleinformatycznym;

3) dokonuje się wyboru metody analizy ryzyka.

4. Kierownik jednostki organizującej system teleinformatyczny odpowiada za zapewnienie ciągłości procesu zarządzania ryzykiem w systemie teleinformatycznym.

5. W sytuacji gdy system teleinformatyczny jest użytkowany przez kilka niezależnych jednostek organizacyjnych, każdy kierownik jednostki organizacyjnej użytkującej system teleinformatyczny współdziała z osobą, o której mowa w ust. 4, w celu zapewnienia ciągłości procesu zarządzania ryzykiem w systemie teleinformatycznym.

§ 20. 1. Szacowanie ryzyka dla bezpieczeństwa informacji niejawnych obejmuje:

1) analizę ryzyka, na którą składają się:

a) identyfikacja ryzyka,

b) określenie wielkości ryzyk;

2) ocenę ryzyka.

2. W ramach identyfikacji ryzyka określa się:

1) zasoby systemu teleinformatycznego;

2) zagrożenia;

3) podatności;

4) zabezpieczenia;

5) skutki wystąpienia incydentu bezpieczeństwa teleinformatycznego.

3. W procesie określania wielkości ryzyk wyznacza się poziomy zidentyfikowanych ryzyk.

4. W procesie oceny ryzyka porównuje się wyznaczone poziomy ryzyk z tymi, które można zaakceptować. Na podstawie oceny podejmuje się decyzję co do dalszego postępowania z ryzykami.

5. Wstępne szacowanie ryzyka dla bezpieczeństwa informacji niejawnych przeprowadza się przed podjęciem decyzji o wprowadzeniu niezbędnych zabezpieczeń w systemie teleinformatycznym.

6. Wyniki wstępnego szacowania ryzyka, o którym mowa w ust. 5:

1) przedstawia się w dokumentacji bezpieczeństwa systemu teleinformatycznego;

2) wykorzystuje się w procesie projektowania zabezpieczeń dla danego systemu teleinformatycznego przeciwdziałających zidentyfikowanym zagrożeniom;

3) zachowuje się na potrzeby przyszłych uaktualnień.

7. Szacowanie ryzyka dla bezpieczeństwa informacji niejawnych przeprowadza się ponownie:

1) w przypadku wprowadzania w systemie teleinformatycznym zmian, które mogą mieć wpływ na bezpieczeństwo przetwarzanych w nim informacji;

2) po wykryciu nowych zagrożeń lub zidentyfikowaniu nowych podatności, które nie były rozpatrywane podczas wcześniejszego szacowania ryzyka dla bezpieczeństwa informacji niejawnych;

3) w przypadku zaistnienia istotnego incydentu bezpieczeństwa teleinformatycznego;

4) jeżeli zmianie lub rozszerzeniu uległo przeznaczenie, zadania lub funkcjonalność systemu teleinformatycznego;

5) okresowo, w ramach procesu zarządzania ryzykiem w systemie teleinformatycznym.

8. Częstotliwość okresowego przeprowadzania szacowania ryzyka, o którym mowa w ust. 7 pkt 5, określa się w dokumentacji bezpieczeństwa systemu teleinformatycznego.

§ 21. 1. W ramach postępowania z ryzykiem możliwe jest:

1) obniżanie ryzyka przez wdrażanie zabezpieczeń;

2) pozostawienie ryzyka na poziomie określonym w procesie szacowania ryzyka i zaniechanie dalszych działań;

3) unikanie ryzyka przez niepodejmowanie działań będących źródłem ryzyka;

4) przeniesienie ryzyka na inny podmiot w zakresie odpowiedzialności za zarządzanie ryzykiem bez możliwości przeniesienia odpowiedzialności za skutki wynikające z naruszenia poufności, integralności lub dostępności informacji niejawnych przetwarzanych w systemie teleinformatycznym.

2. Doboru zabezpieczeń, o których mowa w ust. 1 pkt 1, dokonuje się z uwzględnieniem zaleceń.

3. Dla ryzyk, które nie mogą być zaakceptowane ze względu na ich zbyt wysoki poziom, proces postępowania z ryzykiem przeprowadza się ponownie, analizując inne warianty.

4. Ryzyka pozostające po procesie postępowania z ryzykiem (ryzyka szczątkowe) podlegają procesowi akceptacji ryzyka.

§ 22. Kierownik jednostki organizacyjnej w procesie akceptacji ryzyka dokonuje formalnego zaakceptowania ryzyka szczątkowego wraz z jego ewentualnymi konsekwencjami.

§ 23. Proces przeglądu, monitorowania i informowania o ryzyku przeprowadza się przez:

1) regularny przegląd i udoskonalanie procesu zarządzania ryzykiem w systemie teleinformatycznym w celu zapewnienia jego prawidłowości i skuteczności stosownie do zmieniających się okoliczności;

2) monitorowanie czynników ryzyka w celu wykrycia zmian we wczesnym ich stadium i możliwie szybkim na nie reagowaniu;

3) niezwłoczne przekazywanie informacji o pojawiających się ryzykach osobom odpowiedzialnym za zarządzanie ryzykiem.

§ 24. W procesie zarządzania ryzykiem w systemie teleinformatycznym uwzględnia się zalecenia.

Rozdział 4

Dokumentacja bezpieczeństwa teleinformatycznego

§ 25. 1. Dokument szczególnych wymagań bezpieczeństwa systemu teleinformatycznego:

1) opracowuje się na etapie projektowania systemu teleinformatycznego, po przeprowadzeniu wstępnego szacowania ryzyka dla bezpieczeństwa informacji niejawnych, które mają być przetwarzane w systemie teleinformatycznym, w sposób uwzględniający specyfikę budowy, charakterystykę systemu teleinformatycznego, a także warunki charakterystyczne dla jednostki organizacyjnej;

2) bieżąco uzupełnia się na etapie wdrażania systemu teleinformatycznego, po przeprowadzeniu szacowania ryzyka dla bezpieczeństwa informacji niejawnych z uwzględnieniem wprowadzonych zabezpieczeń;

3) uaktualnia się na etapie eksploatacji systemu teleinformatycznego, przed dokonaniem zmian w systemie teleinformatycznym.

2. Dokument szczególnych wymagań bezpieczeństwa zawiera następujące dane:

1) rodzaje oraz klauzule tajności informacji niejawnych, które będą przetwarzane w systemie teleinformatycznym;

2) grupy użytkowników systemu teleinformatycznego wyodrębnione ze względu na posiadane uprawnienia do pracy w systemie teleinformatycznym;

3) tryb bezpieczeństwa pracy systemu teleinformatycznego;

4) przeznaczenie i funkcjonalność systemu teleinformatycznego;

5) wymagania eksploatacyjne dla wymiany informacji i połączeń z innymi systemami teleinformatycznymi;

6) lokalizację systemu teleinformatycznego.

3. W dokumencie szczególnych wymagań bezpieczeństwa zawiera się ponadto informacje o:

1) metodyce użytej w procesie szacowania ryzyka dla bezpieczeństwa informacji niejawnych oraz raport z tego procesu;

2) zastosowanych zabezpieczeniach;

3) ryzykach szczątkowych oraz deklaracji ich akceptacji;

4) poświadczeniach bezpieczeństwa lub innych formalnych uprawnieniach do dostępu do informacji niejawnych, posiadanych przez użytkowników systemu teleinformatycznego;

5) bezpieczeństwie fizycznym, w tym granicach i lokalizacji stref ochronnych oraz środkach ich ochrony;

6) ochronie elektromagnetycznej;

7) stosowanych urządzeniach lub narzędziach kryptograficznych;

8) ciągłości działania, w tym tworzeniu kopii zapasowych, odzyskiwaniu systemu oraz, jeżeli to właściwe, zapewnieniu alternatywnych łączy telekomunikacyjnych lub urządzeń, a także zasilaniu awaryjnym;

9) ustawieniach konfiguracyjnych systemu teleinformatycznego;

10) utrzymaniu systemu, w tym dokonywaniu przeglądów diagnostycznych i napraw;

11) zapobieganiu incydentom bezpieczeństwa teleinformatycznego, w tym ochronie przed oprogramowaniem złośliwym;

12) zasadach wprowadzania poprawek lub uaktualnień oprogramowania;

13) ochronie nośników, w tym ich oznaczaniu, dostępie, transporcie, obniżaniu ich klauzul tajności i niszczeniu;

14) identyfikacji i uwierzytelnieniu użytkowników i urządzeń;

15) kontroli dostępu;

16) audycie wewnętrznym;

17) zarządzaniu ryzykiem w systemie teleinformatycznym;

18) zmianach w systemie teleinformatycznym, w tym dotyczących aktualizacji dokumentacji bezpieczeństwa systemu teleinformatycznego oraz warunkach ponownej akredytacji systemu teleinformatycznego i wycofania z eksploatacji.

§ 26. 1. Dokument procedur bezpiecznej eksploatacji:

1) opracowuje się na etapie wdrażania systemu teleinformatycznego, po przeprowadzeniu szacowania ryzyka dla bezpieczeństwa informacji niejawnych z uwzględnieniem wprowadzonych zabezpieczeń;

2) uaktualnia się na etapie eksploatacji systemu teleinformatycznego, przed dokonaniem zmian w systemie teleinformatycznym.

2. W dokumencie procedur bezpiecznej eksploatacji określa się szczegółowy wykaz procedur bezpieczeństwa wraz z dokładnym opisem sposobu ich wykonania, realizowanych przez osoby odpowiedzialne za bezpieczeństwo teleinformatyczne oraz osoby uprawnione do pracy w systemie teleinformatycznym, obejmujący:

1) administrowanie systemem teleinformatycznym oraz zastosowanymi środkami zabezpieczającymi;

2) bezpieczeństwo urządzeń;

3) bezpieczeństwo oprogramowania;

4) zarządzanie konfiguracją sprzętowo-programową, w tym zasady serwisowania lub modernizacji oraz wycofywania z użycia elementów systemu teleinformatycznego;

5) plany awaryjne;

6) monitorowanie i audyt systemu teleinformatycznego;

7) zarządzanie nośnikami;

8) zarządzanie materiałami kryptograficznymi;

9) stosowanie ochrony elektromagnetycznej;

10) reagowanie na incydenty bezpieczeństwa teleinformatycznego;

11) szkolenia użytkowników systemu teleinformatycznego dotyczące zasad korzystania z systemu teleinformatycznego;

12) wprowadzanie danych do systemu i ich wyprowadzanie z systemu.

§ 27. W przypadku systemu teleinformatycznego funkcjonującego w więcej niż jednej jednostce organizacyjnej, po uzgodnieniu z jednostką organizującą system, dokumentacja bezpieczeństwa systemu teleinformatycznego może być uzupełniona o aneksy zawierające dane dotyczące konkretnych lokalizacji, sporządzane przez kierowników jednostek organizacyjnych, w których znajdują się elementy systemu teleinformatycznego.

Rozdział 5

Przepis końcowy

§ 28. Rozporządzenie wchodzi w życie po upływie 14 dni od dnia ogłoszenia.[1)]

Prezes Rady Ministrów: *D. Tusk*

[1)] Niniejsze rozporządzenie było poprzedzone rozporządzeniem Prezesa Rady Ministrów z dnia 25 sierpnia 2005 r. w sprawie podstawowych wymagań bezpieczeństwa teleinformatycznego (Dz. U. Nr 171, poz. 1433), które traci moc z dniem wejścia w życie niniejszego rozporządzenia na podstawie art. 189 ust. 1 ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. Nr 182, poz. 1228).