24.01.2011

ROZPORZĄDZENIE
PREZESA RADY MINISTRÓW

z dnia .....

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 (Dz. U. Nr 182, poz. 1228), 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 założonym czasie, przez podmiot uprawniony do pracy w systemie teleinformatycznym;

2) incydencie bezpieczeństwa teleinformatycznego – należy przez to rozumieć każde zdarzenie, które może mieć negatywny wpływ na bezpieczeństwo zasobów systemu teleinformatycznego, spowodowane w szczególności awarią systemu teleinformatycznego, działaniem osób uprawnionych lub nieuprawnionych do pracy w tym systemie teleinformatycznym albo zaniechaniem osób uprawnionych;

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

www.inforlex.pl

4) informatycznym nośniku danych – należy przez to rozumieć informatyczny nośnik danych w rozumieniu art. 3 pkt 1 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2005 r., nr 64, poz. 565);

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

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

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

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

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

10) ryzyku – ryzyko, o którym mowa w art. 2 pkt 15 ustawy;

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

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

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

14) zasobach systemu teleinformatycznego – należy przez to rozumieć przetwarzane w systemie teleinformatycznym informacje niejawne, jak również 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

www.inforlex.pl

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

§ 4. 1. Organizowanie systemów teleinformatycznych przez Organizację Traktatu Północnoatlantyckiego, Unię Europejską lub inne organizacje międzynarodowe odbywa się zgodnie z wymaganiami bezpieczeństwa teleinformatycznego określonymi przez daną organizację międzynarodową.

2. Organizowanie systemów teleinformatycznych przeznaczonych do przetwarzania informacji niejawnych międzynarodowych, organizowanych przez polskie jednostki organizacyjne, odbywa się z uwzględnieniem wymagań wynikających z umów międzynarodowych.

www.inforlex.pl

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 poprzez:

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) weryfikację zabezpieczeń, polegającą na okresowym sprawdzaniu poprawności działania i skuteczności wdrożonych zabezpieczeń;

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

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

§ 6. 1. Systemy teleinformatyczne, w których przetwarzane są informacje niejawne chroni się przed nieuprawnionym dostępem.

www.inforlex.pl

2. W celu zapewnienia ochrony przed nieuprawnionym dostępem do systemu teleinformatycznego w szczególności:

   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 instaluje się je w sposób zapewniający możliwość wykrycia prób fizycznego dostępu lub wprowadzenia nieuprawnionych zmian.

§ 7. 1. Ochronę elektromagnetyczną systemu teleinformatycznego stosuje się w celu niedopuszczenia do utraty dostępności lub poufności informacji niejawnych w urządzeniach teleinformatycznych, następującej w szczególności na skutek:

   1) zakłócania pracy urządzeń teleinformatycznych za pomocą emisji lub impulsów elektromagnetycznych o dużej mocy – w przypadku zagrożenia utratą dostępności;

   2) wykorzystania elektromagnetycznej emisji ujawniającej informacje przetwarzane w systemie teleinformatycznym pochodzącej z tych urządzeń – w przypadku zagrożenia utratą poufności.

2. Ochronę elektromagnetyczną systemu teleinformatycznego zapewnia się w szczególności przez umieszczenie urządzeń teleinformatycznych, połączeń i linii w strefach spełniających wymagania w zakresie tłumienności elektromagnetycznej lub zastosowanie odpowiednich urządzeń teleinformatycznych, połączeń i linii o obniżonym poziomie emisji lub ich ekranowanie z jednoczesnym filtrowaniem zewnętrznych linii zasilających i sygnałowych.

3. Środki ochrony przed utratą dostępności, o której mowa w ust. 1 pkt 1, dobiera się z uwzględnieniem wyników szacowania ryzyka dla bezpieczeństwa informacji niejawnych.

4. W systemie teleinformatycznym przetwarzającym informacje niejawne o klauzuli „poufne" lub wyższej, środki ochrony przed utratą poufności, o której mowa w ust. 1 pkt 2, zapewnia się na podstawie zaleceń, o których mowa w art. 52 ust. 3 ustawy, zwanych dalej „zaleceniami", z uwzględnieniem wyników szacowania ryzyka dla bezpieczeństwa informacji niejawnych.

www.inforlex.pl

§ 8. 1. W celu zapewnienia dostępności zasobów w systemie teleinformatycznym wprowadza się w szczególności:

1) zasady tworzenia i przechowywania kopii zapasowych;
2) procedury postępowania w sytuacjach kryzysowych, w tym w przypadkach awarii elementów systemu teleinformatycznego;
3) monitorowanie stanu technicznego i wydajności systemu teleinformatycznego.

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

§ 9. 1. W zależności od potrzeb oraz wyników szacowania ryzyka dla bezpieczeństwa informacji niejawnych, transmisję danych w systemie teleinformatycznym chroni się przed wykryciem, przechwyceniem lub zakłócaniem, stosując w szczególności:

1) maskowanie ruchu;
2) zmianę parametrów transmisji.

2. Poufność informacji niejawnych przekazywanych w formie transmisji poza strefami ochronnymi zapewnia się w szczególności poprzez stosowanie certyfikowanych urządzeń lub narzędzi kryptograficznych.

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 innymi zabezpieczeniami.

§ 10. W systemie teleinformatycznym przetwarzającym informacje niejawne tworzy się i przechowuje rejestry zdarzeń, a także zapewnia ich integralność i dostępność, w zakresie niezbędnym do zapewnienia przeglądu, analizy oraz dostarczania dowodów działań naruszających bezpieczeństwo informacji.

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

www.inforlex.pl

§ 12. 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.

§ 13. Inspektor bezpieczeństwa teleinformatycznego bierze udział w procesie zarządzania ryzykiem w systemie teleinformatycznym oraz w tworzeniu dokumentacji bezpieczeństwa systemu teleinformatycznego, a w ramach bieżącej kontroli zgodności funkcjonowania systemu teleinformatycznego ze szczególnymi wymaganiami bezpieczeństwa oraz przestrzegania procedur bezpiecznej eksploatacji sprawdza:

1) poprawność realizacji zadań przez administratora, w szczególności 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 szczególności w zakresie wykorzystywania urządzeń i narzędzi służących do ochrony informacji niejawnych;
3) stan zabezpieczeń systemu teleinformatycznego, w szczególności analizując rejestry zdarzeń systemu teleinformatycznego.

§ 14. Administrator systemu teleinformatycznego, w ramach odpowiedzialności za jego funkcjonowanie oraz przestrzeganie zasad i wymagań bezpieczeństwa dla systemu teleinformatycznego, w szczególności:

1) bierze udział w procesie zarządzania ryzykiem w systemie teleinformatycznym oraz w tworzeniu dokumentacji bezpieczeństwa systemu teleinformatycznego;
2) prowadzi szkolenia użytkowników systemu teleinformatycznego;
3) utrzymuje zgodność systemu teleinformatycznego z jego dokumentacją bezpieczeństwa;
4) wdraża zabezpieczenia w systemie teleinformatycznym.

§ 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

www.inforlex.pl

wyższej klauzuli tajności do systemu teleinformatycznego przetwarzającego informacje o klauzuli niższej.

§ 16. Urządzenie lub narzędzie przeznaczone do ochrony informacji niejawnych, dla którego został wydany przez Agencję Bezpieczeństwa Wewnętrznego, zwaną dalej „ABW", lub Służbę Kontrwywiadu Wojskowego, zwaną dalej „SKW", certyfikat ochrony kryptograficznej lub elektromagnetycznej, podlega ochronie do momentu jego zniszczenia.

§ 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 certyfikowanych urządzeń lub narzędzi kryptograficznych, 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. Możliwość obniżenia lub zniesienia klauzuli tajności, sposób przeprowadzania procesu trwałego usuwania danych oraz sposób niszczenia informatycznych nośników danych uzgadnia się z ABW lub SKW.

§ 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.

www.inforlex.pl

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:

www.inforlex.pl

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, jeśli 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.

6. Na etapie wycofywania:

1) zaprzestaje się eksploatacji systemu teleinformatycznego;

2) powiadamia się ABW albo SKW o fakcie wycofania systemu teleinformatycznego 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 poprzez przeniesienie ich do innego systemu teleinformatycznego, zarchiwizowanie lub zniszczenie informatycznych nośników danych.

Rozdział 3

Zarządzanie ryzykiem w systemie teleinformatycznym

§ 19. 1. Zarządzanie ryzykiem w systemie teleinformatycznym prowadzi się realizując procesy:

1) szacowania ryzyka dla bezpieczeństwa informacji niejawnych;

www.inforlex.pl

2) postępowania z ryzykiem;

3) akceptacji ryzyka;

4) przeglądu i monitorowania ryzyka.

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

3. 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. 2 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) estymacja ryzyka,

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 estymacji ryzyka 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;

www.inforlex.pl

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) jeśli 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:

1) obniża się ryzyko poprzez wdrażanie zabezpieczeń;

2) pozostawia się ryzyko na poziomie określonym w trakcie estymacji ryzyka i zaniechanie dalszych działań;

3) unika się ryzyka poprzez niepodejmowanie działań będących źródłem ryzyka;

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.

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

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

www.inforlex.pl

§ 23. Proces przeglądu i monitorowania ryzyka przeprowadza się przez:

1) monitorowanie czynników ryzyka w celu wykrycia zmian we wczesnym ich stadium i możliwie szybkim na nie reagowaniu;
2) regularny przegląd i udoskonalanie procesu zarządzania ryzykiem w systemie teleinformatycznym w celu zapewnienia jego prawidłowości i skuteczności stosownie do zmieniających się okoliczności.

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

Rozdział 4

Dokumentacja bezpieczeństwa teleinformatycznego

§ 25. 1. Dokument szczególnych wymagań bezpieczeństwa systemu teleinformatycznego opracowuje się po przeprowadzeniu szacowania ryzyka dla bezpieczeństwa informacji niejawnych, które mają być przetwarzane w systemie teleinformatycznym, z uwzględnieniem warunków charakterystycznych dla jednostki organizacyjnej.

2. Sporządzanie dokumentu szczególnych wymagań bezpieczeństwa zaczyna się od wstępnej, zwięzłej i jednoznacznej definicji systemu teleinformatycznego obejmującej następujące aspekty:

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.

www.inforlex.pl

3. W dokumencie szczególnych wymagań bezpieczeństwa zawiera się informację o metodyce użytej w procesie szacowania ryzyka dla bezpieczeństwa informacji niejawnych, raport z tego procesu, opis zastosowanych zabezpieczeń, opis ryzyk szczątkowych oraz deklarację ich akceptacji, a ponadto odnosi się do następujących zagadnień:

1) poświadczeń bezpieczeństwa lub innych formalnych uprawnień do dostępu do informacji niejawnych, posiadanych przez użytkowników systemu teleinformatycznego;
2) bezpieczeństwa fizycznego, w tym granic i lokalizacji stref ochronnych oraz środków ich ochrony;
3) ochrony elektromagnetycznej;
4) stosowanych urządzeń i narzędzi kryptograficznych;
5) ciągłości działania, w tym tworzenia kopii zapasowych, odzyskiwania systemu oraz, jeżeli to właściwe, zapewnienia alternatywnych łączy telekomunikacyjnych i urządzeń, a także zasilania awaryjnego;
6) ustawień konfiguracyjnych systemu teleinformatycznego;
7) utrzymania systemu, w tym dokonywania przeglądów diagnostycznych i napraw;
8) integralności systemu teleinformatycznego;
9) zapobiegania incydentom bezpieczeństwa teleinformatycznego, w tym ochrony przed oprogramowaniem złośliwym;
10) zasad wprowadzania poprawek lub uaktualnień oprogramowania;
11) ochrony nośników, w tym ich oznaczania, dostępu, transportu, obniżania ich klauzul tajności i niszczenia;
12) identyfikacji i uwierzytelnienia użytkowników i urządzeń;
13) kontroli dostępu;
14) audytu wewnętrznego;
15) zarządzania ryzykiem w systemie teleinformatycznym;
16) zmian w systemie teleinformatycznym, w tym dotyczących aktualizacji dokumentacji bezpieczeństwa systemu teleinformatycznego oraz warunków ponownej akredytacji systemu teleinformatycznego i wycofania z eksploatacji;

§ 26. 1. W procedurach bezpiecznej eksploatacji określa się szczegółowy wykaz

www.inforlex.pl

czynności wraz z dokładnym opisem sposobu ich wykonania, realizowanych przez osoby odpowiedzialne za bezpieczeństwo teleinformatyczne oraz osoby uprawnione do pracy w systemie teleinformatycznym.

2. Szczegółowy wykaz czynności ujmuje się w tematycznie wyodrębnione procedury bezpieczeństwa, obejmujące następujące zagadnienia:

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.

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

www.inforlex.pl

Rozdział 5

Przepis końcowy

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

Prezes Rady Ministrów

[1)] Niniejsze rozporządzenie było poprzedzone rozporządzeniem Prezesa Rady Ministrów z dnia 25 sierpnia 2005 r. w sprawie podstawowych wymagań bezpieczeństwa teleinformatycznego (Dz. U. z 2005 r., 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).

www.inforlex.pl

UZASADNIENIE

Rozporządzenie Prezesa Rady Ministrów w sprawie podstawowych wymagań bezpieczeństwa teleinformatycznego stanowi wykonanie upoważnienia ustawowego wynikającego z art. 49 ust. 9 ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. Nr 182, poz. 1228), zwanej dalej „ustawą".

Problematyka stanowiąca materię normatywną projektu jest aktualnie uregulowana w rozporządzeniu Prezesa Rady Ministrów z dnia 25 sierpnia 2005 r. w sprawie podstawowych wymagań bezpieczeństwa teleinformatycznego (Dz. U. Nr 171, poz. 1433).

Proponowane rozporządzenie ma na celu określenie, ujednolicenie oraz doprecyzowanie podstawowych wymagań bezpieczeństwa dla systemów teleinformatycznych służących do przetwarzania informacji niejawnych, przez co ułatwi oraz usprawni organizację systemu teleinformatycznego i tworzenie dokumentacji bezpieczeństwa teleinformatycznego, zgodnie z nowymi przepisami ustawowymi. Obejmuje ono również unormowanie stosowania spójnego zbioru zabezpieczeń w celu zapewnienia ochrony informacji niejawnych przetwarzanych w systemach teleinformatycznych przed utratą poufności, integralności i dostępności, mogących zaistnieć w wyniku przypadku lub celowych działań.

W przedmiotowym projekcie rozporządzenia uszczegółowiono podstawowe wymagania bezpieczeństwa teleinformatycznego oraz treść przepisów dotyczących dokumentacji bezpieczeństwa teleinformatycznego. Określając wymagania bezpieczeństwa uwzględniono regulacje zawarte w dokumentach normatywnych UE i NATO (Security within The North Atlantic Trean Organisation (NATO) C-M(2002)49, Decyzja Rady Unii Europejskiej z dnia 19 marca 2001 r. w sprawie przyjęcia przepisów Rady dotyczących bezpieczeństwa) oraz wytyczne amerykańskiego National Institute of Standards and Technology (NIST) odnoszące się do bezpieczeństwa systemów teleinformatycznych (w szczególności dokument „Special Publication 800-53" wykorzystany jako pomocniczy wzorzec sprawdzonych rozwiązań dotyczących regulowanej rozporządzeniem materii). Szczególny nacisk położono na fakt, iż bezpieczeństwo informacji niejawnych przetwarzanych w systemie teleinformatycznym musi być uwzględnione w całym cyklu życia systemu teleinformatycznego, który to cykl szczegółowo unormowano w § 18.

Istotnym novum tego projektu rozporządzenia jest rozdział 3, zawierający przepisy dotyczące zarządzania ryzykiem w systemie teleinformatycznym, określające jego

www.inforlex.pl

poszczególne procesy oraz sposób ich realizacji. Sposób zarządzania ryzykiem w systemie teleinformatycznym oparto o Polską Normę PN-ISO/IEC 27005:2010.

Należy wyraźnie podkreślić, że szacownie ryzyka dla bezpieczeństwa informacji niejawnych jest jednym z trzech najważniejszych, obok uwarunkowań wynikających z obowiązujących przepisów prawnych i zaleceń w zakresie bezpieczeństwa teleinformatycznego, środków ochrony systemu teleinformatycznego. Stąd, wprowadzenie takiego uregulowania ma na celu zapewnienie doboru zabezpieczeń służących ochronie sytemu teleinformatycznego w sposób spójny i racjonalny.

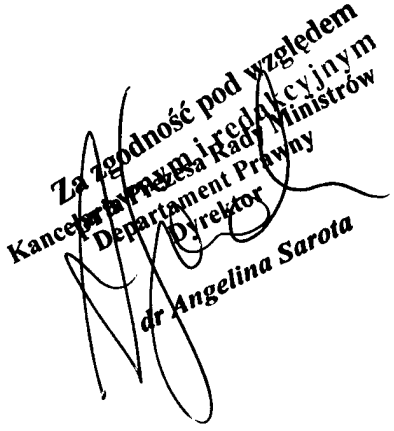
W myśl proponowanych uregulowań, za zapewnienie ciągłości procesu zarządzania ryzykiem w systemie teleinformatycznym, odpowiada kierownik jednostki organizacyjnej organizującej ten system, a w przypadku, gdy system teleinformatyczny jest użytkowany przez kilka niezależnych jednostek organizacyjnych – każdy kierownik jednostki organizacyjnej użytkującej system teleinformatyczny, współdziałając z innymi kierownikami jednostek organizacyjnych, w celu zapewnienia ciągłości procesu zarządzania ryzykiem w systemie teleinformatycznym.

Projekt rozporządzenia stanowi rozwinięcie zawartej w nowej ustawie o ochronie informacji niejawnych zasady, zgodnie z którą szacowanie ryzyka dla bezpieczeństwa informacji niejawnych stało się podstawą określenia niezbędnych elementów bezpieczeństwa teleinformatycznego. To właśnie na podstawie wyników szacowania ryzyka dla bezpieczeństwa informacji niejawnych będzie można określić, które zabezpieczenia są niezbędne, a które można zastąpić innymi (w tym np. tańszymi) rozwiązaniami zakładając, że ryzyko szczątkowe z nimi związane będzie mogło być zaakceptowane. Powyższe rozwiązanie (dzięki zastosowaniu elastycznego i indywidualnego podejścia do każdego organizowanego systemu teleinformatycznego) może mieć więc korzystny wpływ na kwestie związane z kosztami organizacji bezpieczeństwa teleinformatycznego.

W stosunku do poprzedniego stanu prawnego, rozdział 4, regulujący zagadnienia związane z dokumentacją bezpieczeństwa teleinformatycznego, został znacznie rozszerzony i uszczegółowiony, przy czym duży nacisk położono w nim na zgodność z obowiązującymi w tym zakresie uregulowaniami UE i NATO. W rozdziale tym usystematyzowano m. in. wymagania dotyczące zawartości dokumentacji bezpieczeństwa, warunkującej możliwość akredytacji systemu teleinformatycznego oraz sprawowania późniejszego nadzoru w celu zapewnienia bezpieczeństwa przetwarzanym w nim informacjom niejawnym.

www.inforlex.pl

Zgodnie z art. 5 ustawy z dnia 7 lipca 2005 r. o działalności lobbingowej w procesie stanowienia prawa (Dz. U. Nr 169, poz. 1414 oraz z 2009 r. Nr 42, poz. 337), projekt rozporządzenia został udostępniony w Biuletynie Informacji Publicznej na stronie podmiotowej Kancelarii Prezesa Rady Ministrów



www.inforlex.pl

Ocena Skutków Regulacji (OSR)

1. **Podmioty, na które oddziałuje rozporządzenie**

Zakres oddziaływania przepisów rozporządzenia jest ograniczony do podmiotów zainteresowanych uzyskaniem świadectwa akredytacji bezpieczeństwa systemu teleinformatycznego. Projekt zostanie skierowany do konsultacji z organizacjami zrzeszającymi pełnomocników do spraw ochrony informacji niejawnych oraz specjalistów z zakresu bezpieczeństwa systemów teleinformatycznych.

2. **Wpływ regulacji na sektor finansów publicznych, w tym na budżet państwa i budżety jednostek samorządu terytorialnego**

Wejście w życie rozporządzenia nie będzie miało wpływu na budżet państwa i budżet jednostek samorządu terytorialnego.

3. **Wpływ regulacji na rynek pracy**

Wejście w życie rozporządzenia nie będzie miało wpływu na rynek pracy.

4. **Wpływ regulacji na konkurencyjność gospodarki i przedsiębiorczość, w tym na funkcjonowanie przedsiębiorstw**

Wejście w życie rozporządzenia nie wpłynie na konkurencyjność, zarówno wewnętrzną, jak i zewnętrzną gospodarki.

5. **Wpływ regulacji na sytuację i rozwój regionalny**

Wejście w życie rozporządzenia pozostanie bez wpływu na sytuację i rozwój regionalny.

6. **Zgodność z przepisami prawa Unii Europejskiej**

Przedmiotowe rozporządzenie nie jest objęte zakresem Unii Europejskiej. W związku z tym projekt nie został przedstawiony właściwym instytucjom i organom Unii Europejskiej lub Europejskiemu Bankowi Centralnemu celem uzyskania opinii, dokonania konsultacji albo uzgodnienia. Projekt rozporządzenia nie zawiera przepisów technicznych i w związku z tym nie podlega procedurze notyfikacji aktów prawnych, określonej w rozporządzeniu Rady Ministrów z dnia 23 grudnia 2002r. w sprawie sposobu funkcjonowania krajowego systemu notyfikacji norm i aktów prawnych (Dz.U. Nr 239, poz. 2039 i z 2004r. Nr 65, poz. 597).

Za zgodność pod względem prawnym i redakcyjnym
Kancelaria Prezesa Rady Ministrów
Departament Prawny
Dyrektor
dr Angelina Sarota
www.inforlex.pl