BEZPIECZEŃSTWO TELEINFORMATYCZNE

Dopuszczenie systemu teleinformatycznego do przetwarzania informacji niejawnych

Art. 48.

1. **Systemy teleinformatyczne, w których mają być przetwarzane informacje niejawne, podlegają akredytacji bezpieczeństwa teleinformatycznego.**
2. **Akredytacji, o której mowa w ust. 1, udziela się na czas określony, nie dłuższy niż 5 lat.**

Dopuszczenie do przetwarzania informacji niejawnych

Akredytacja w terminie 6 miesięcy

Akredytacja systemów teleinformatycznych przeznaczonych do przetwarzania informacji niejawnych krajowych o klauzuli zastrzeżone		Akredytacja systemów teleinformatycznych przeznaczonych do przetwarzania informacji niejawnych krajowych o klauzulach poufne, tajne i ściśle tajne lub/i NATO, UE, ESA – wszystkie klauzule	
Etap I:	Opracowanie dokumentacji bezpieczeństwa.	**Etap I:**	Opracowanie dokumentacji bezpieczeństwa.
Etap II:	Udzielenie akredytacji bezpieczeństwa teleinformatycznego przez kierownika jednostki organizacyjnej.	**Etap II:**	Przesłanie dokumentacji bezpieczeństwa systemu do ABW lub SKW.
Etap III:	Możliwość rozpoczęcia przetwarzania informacji niejawnych.	**Etap III:**	Przeprowadzenie oceny bezpieczeństwa systemu TI na podstawie dokumentacji bezpieczeństwa.
Etap IV:	Przesłanie dokumentacji bezpieczeństwa systemu do ABW lub SKW.	**Etap IV:**	Zatwierdzenie przez ABW lub SKW dokumentacji bezpieczeństwa systemu/ew. wniesienie uwag.
Etap V*:	Przedstawienie kierownikowi jednostki organizacyjnej, przez ABW lub SKW ewentualnych zaleceń. W szczególnych przypadkach wstrzymanie pracy systemu.	**Etap V:**	Przesłanie do ABW wniosku o audyt bezpieczeństwa teleinformatycznego (WA-01). lub zgłoszenie gotowości do inspekcji.
Etap VI*:	Zaprzestanie przetwarzania informacji niejawnych.	**Etap VI:**	Audyt bezpieczeństwa systemu teleinformatycznego.
Etap VII*:	Realizacja zaleceń ABW lub SKW. Uzupełnienie dokumentacji bezpieczeństwa.	**Etap VII:**	Opłacenie rachunku za czynność związane z przeprowadzeniem akredytacji.
Etap VIII*:	Przesłanie informacji o realizacji zaleceń lub poprawionej dokumentacji bezpieczeństwa	**Etap VIII:**	Wydanie świadectwa akredytacji systemu teleinformatycznego.
Etap IX*:	Informacja ABW lub SKW o braku przeciwskazań do pracy systemu.	**Etap IX:**	Rozpoczęcie przetwarzania informacji niejawnych.
Etap X*:	Rozpoczęcie przetwarzania informacji niejawnych.		

Akredytacja w terminie 6 miesięcy

* - etap występujący w przypadku wydania przez ABW lub SKW zaleceń dotyczących przeprowadzenia dodatkowych czynności związanych z bezpieczeństwem informacji niejawnych lub wstrzymania systemu.

Dopuszczenie do przetwarzania informacji niejawnych

Akredytacja systemów teleinformatycznych przeznaczonych do przetwarzania informacji niejawnych o klauzuli zastrzeżone oraz NATO , UE i ESA – o klauzulach restricted

Akredytacja w terminie 6 miesięcy

Etap I:	Opracowanie dokumentacji bezpieczeństwa.
Etap II:	Udzielenie akredytacji bezpieczeństwa teleinformatycznego przez kierownika jednostki organizacyjnej (w zakresie przetwarzania informacji krajowych o klauzuli **zastrzeżone**).
Etap III:	Przesłanie dokumentacji bezpieczeństwa systemu do ABW lub SKW.
Etap IV:	Przeprowadzenie oceny bezpieczeństwa systemu TI na podstawie dokumentacji bezpieczeństwa.
Etap V:	Zatwierdzenie przez ABW lub SKW dokumentacji bezpieczeństwa systemu w zakresie **NATO, UE, ESA**
Etap VI:	Zgłoszenie gotowości do **inspekcji**.
Etap VII:	**Inspekcja** systemu teleinformatycznego.
Etap VIII:	Udzielenie akredytacji dla systemu teleinformatycznego w zakresie przetwarzania informacji niejawnych **NATO, UE, ESA** o klauzuli restricted.
Etap IX:	Rozpoczęcie przetwarzania informacji niejawnych.

Akredytacja w terminie 6 miesięcy

Etapy funkcjonowania systemu teleinformatycznego (1/5)

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.

Etapy funkcjonowania systemu teleinformatycznego (2/5)

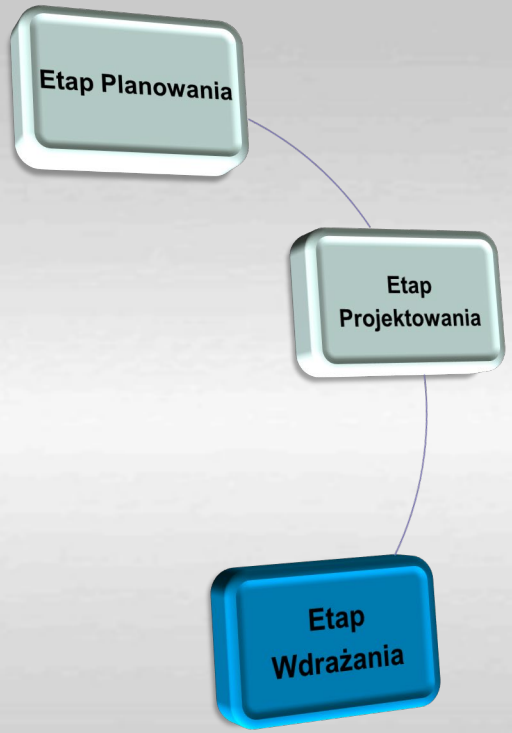
Na etapie projektowania:

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.

Etapy funkcjonowania systemu teleinformatycznego (3/5)

Na etapie wdrażania:

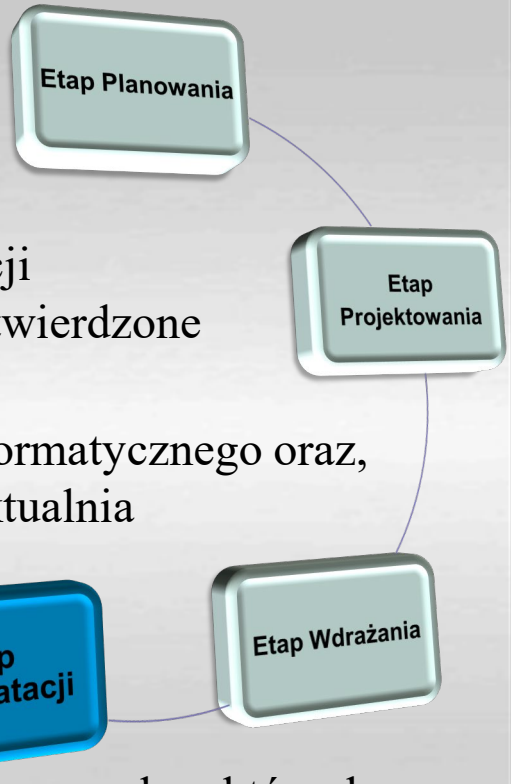
1) pozyskuje i wdraża się urządzenia lub narzędzia realizujące zabezpieczenia w systemie teleinformatycznym;
2) przeprowadza się testy bezpieczeństwa systemu teleinformatycznego;
3) przeprowadza się szacowanie ryzyka dla bezpieczeństwa informacji niejawnych z uwzględnieniem wprowadzonych zabezpieczeń;
4) opracowuje się dokument procedur bezpiecznej eksploatacji oraz uzupełnia dokument szczególnych wymagań bezpieczeństwa;
5) system teleinformatyczny poddaje się akredytacji bezpieczeństwa teleinformatycznego.



Etapy funkcjonowania systemu teleinformatycznego (4/5)

Na etapie eksploatacji:

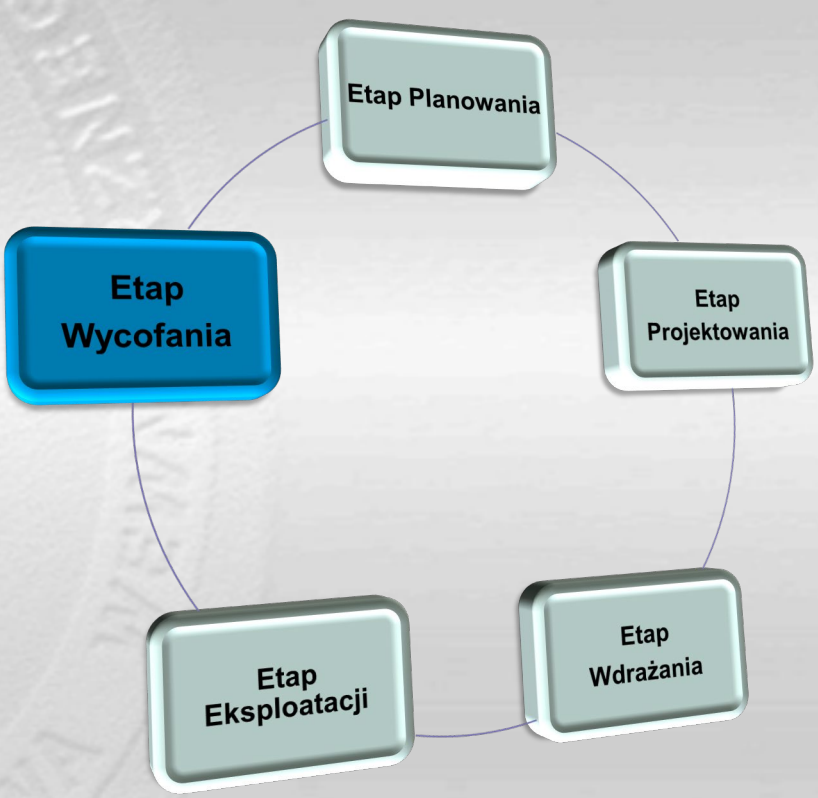
1) utrzymuje się zgodność systemu teleinformatycznego z jego dokumentacją bezpieczeństwa;
2) zapewnia się ciągłość procesu zarządzania ryzykiem w systemie teleinformatycznym;
3) okresowo przeprowadza się testy bezpieczeństwa w celu weryfikacji poprawności działania poszczególnych zabezpieczeń oraz usuwa 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.



Etapy funkcjonowania systemu teleinformatycznego (5/5)

Na etapie wycofania:

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.



Dokumentacja Bezpieczeństwa

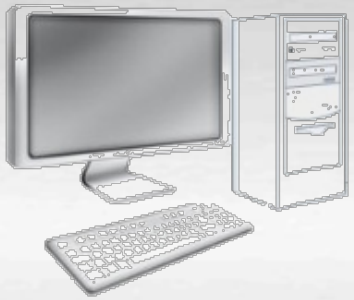
Art. 2.

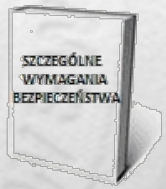
9. Dokumentacją bezpieczeństwa systemu teleinformatycznego – jest dokument szczególnych wymagań bezpieczeństwa oraz dokument procedur bezpiecznej eksploatacji systemu teleinformatycznego, opracowane zgodnie z zasadami określonymi w ustawie;

Liczba dokumentów tworzących dokumentację bezpieczeństwa uzależniona jest od stopnia skomplikowania budowy systemu teleinformatycznego:

W „wariancie podstawowym” w skład dokumentacji bezpieczeństwa wchodzą:

1. Dokument szczególnych wymagań bezpieczeństwa,
2. Dokument procedur bezpiecznej eksploatacji systemu teleinformatycznego.



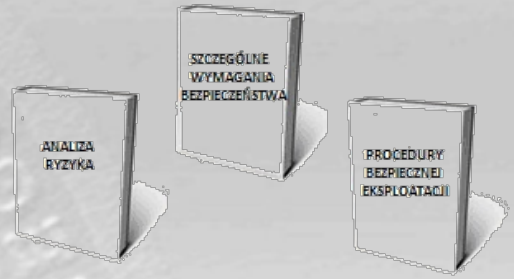


Art. 49.

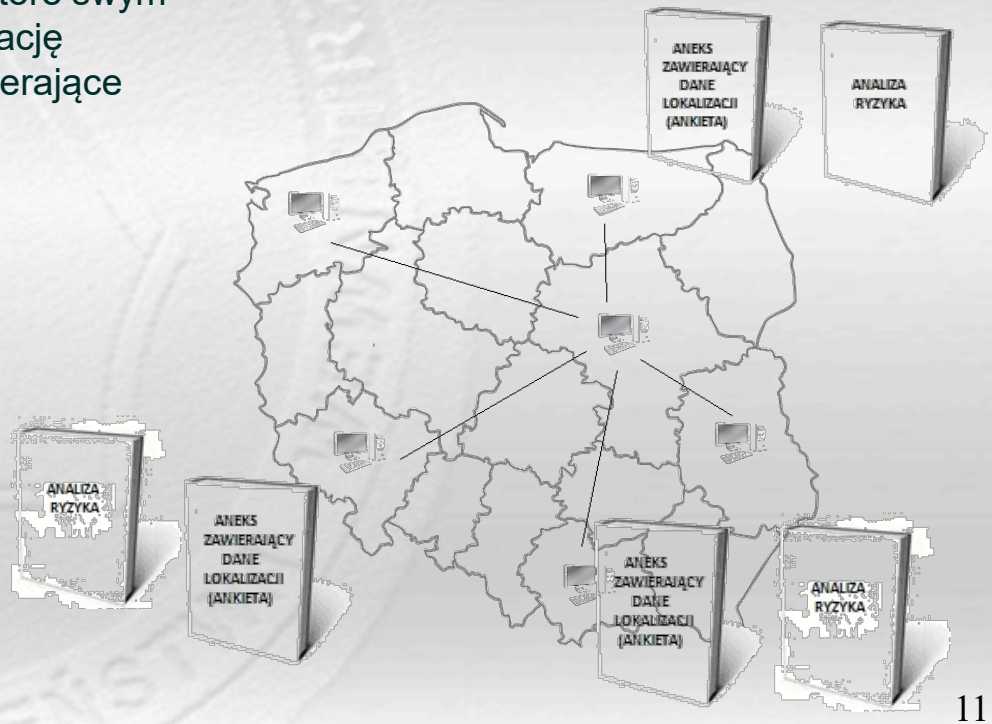
1. (…) Przebieg i wyniki procesu szacowania ryzyka mogą zostać przedstawione w odrębnym dokumencie niż dokument szczególnych wymagań bezpieczeństwa.

Dokumentacja Bezpieczeństwa

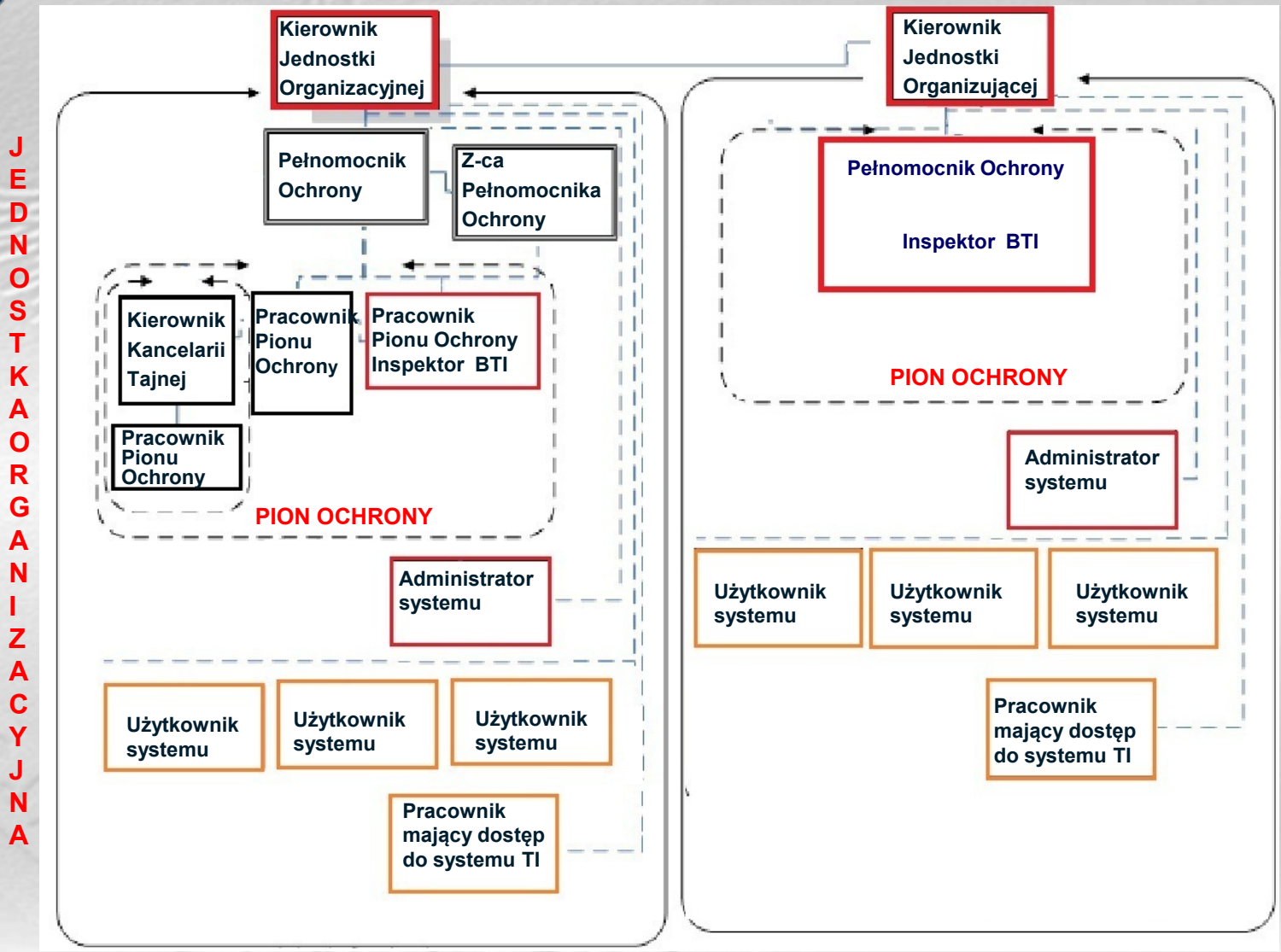
W przypadku obszernych opracowań wynikających ze stopnia skomplikowania systemu, „Przebieg i wyniki procesu szacowania ryzyka” może stanowić osobny dokument.



W przypadku systemów teleinformatycznych, które swym zasięgiem obejmują wiele lokalizacji dokumentację bezpieczeństwa uzupełnia się o: „Aneksy zawierające dane dotyczące konkretnych lokalizacji”.



Struktura organizacyjna



Zakres tematyczny dokumentu szczególnych wymagań bezpieczeństwa

Art. 49.

1. Dokument szczególnych wymagań bezpieczeństwa systemu teleinformatycznego powinien zawierać w szczególności wyniki procesu szacowania ryzyka dla bezpieczeństwa informacji niejawnych przetwarzanych w systemie teleinformatycznym oraz określać przyjęte w ramach zarządzania ryzykiem sposoby osiągania i utrzymywania odpowiedniego poziomu bezpieczeństwa systemu, a także opisywać aspekty jego budowy, zasady działania i eksploatacji, które mają związek z bezpieczeństwem systemu lub wpływają na jego bezpieczeństwo.

§ 25. 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.

Zakres tematyczny dokumentu szczególnych wymagań bezpieczeństwa

§ 25. 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.

Zakres tematyczny dokumentu szczególnych wymagań bezpieczeństwa

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.

Struktura dokumentu szczególnych wymagań bezpieczeństwa - Zalecenia

Nazwa rozdziału	Załącznik
Rozdział nr 1: Wprowadzenie.	
Rozdział nr 2: Charakterystyka systemu TI.	**Zał. nr 1 -** Schemat architektury systemu TI. **Zał. nr 2 -** Wykaz urządzeń. **Zał. nr 3 -** Metryka systemu.
Rozdział nr 3: Metodyka szacowania ryzyka, raport z procesu szacowania ryzyka.	**Zał. nr 4 -** Raport z procesu szacowania ryzyka.
Rozdział nr 4: Bezpieczeństwo osobowe, uprawnienia dostępu do informacji niejawnych.	
Rozdział nr 5 Bezpieczeństwo fizyczne systemu, strefy ochronne i ich zabezpieczenia.	**Zał. nr 5 -** Schemat obrazujący usytuowanie systemu TI.

Struktura dokumentu szczególnych wymagań bezpieczeństwa - Zalecenia

Nazwa rozdziału	Załącznik
Rozdział nr 6: Ochrona elektromagnetyczna.	**Zał. nr 6 -** Kopie certyfikatów ochrony elektromagnetycznej (SSOE i sprzęt).
Rozdział nr 7: Stosowane urządzenia i narzędzia kryptograficzne.	**Zał. nr 7 -** Kopie certyfikatów ochrony kryptograficznej.
Rozdział nr 8: Ciągłość działania, alternatywne łącza telekomunikacyjne, zasilanie awaryjne.	
Rozdział nr 9: Ustawienia konfiguracyjne systemu i urządzeń, zarządzanie konfiguracją.	**Zał. nr 8 -** Opis konfiguracji systemu operacyjnego. **Zał. nr 9 -** Wykaz oprogramowania wykorzystywanego w systemie.

Struktura dokumentu szczególnych wymagań bezpieczeństwa - Zalecenia

Nazwa rozdziału	Załącznik
Rozdział nr 10: Utrzymanie systemu, przeglądy diagnostyczne i naprawy.	
Rozdział nr 11: Zapobieganie i reagowanie na incydenty bezpieczeństwa teleinformatycznego.	
Rozdział nr 12: Zasady wprowadzania poprawek, aktualizacja oprogramowania.	
Rozdział nr 13: Ochrona informatycznych nośników danych wykorzystywanych w systemie.	
Rozdział nr 14: Identyfikacja i uwierzytelnianie użytkowników i urządzeń.	
Rozdział nr 15: Kontrola dostępu do systemu.	**Zał. nr 10 -** Schemat logicznego przepływu informacji (diagram).

Struktura dokumentu szczególnych wymagań bezpieczeństwa - Zalecenia

Nazwa rozdziału	Załącznik
Rozdział nr 16: Audyt wewnętrzny, testy bezpieczeństwa systemu.	**Zał. nr 11 -** Kwestionariusz audytu wewnętrznego systemu TI.
Rozdział nr 17: Zarządzanie ryzykiem w systemie.	
Rozdział nr 18: Wprowadzanie zmian w systemie TI, w dokumentacji bezpieczeństwa systemu. Warunki utrzymania lub ponownej akredytacji systemu TI oraz wycofania systemu TI z eksploatacji.	
Rozdział nr 19: Zespół ds. zarządzania bezpieczeństwem systemu.	

Zakres tematyczny dokumentu procedur bezpiecznej eksploatacji

Art. 49.

Treść dokumentu procedur bezpiecznej eksploatacji określa sposób zarządzania oraz postępowania we wszelkich sprawach związanych z bezpieczeństwem systemu teleinformatycznego wraz ze wskazaniem zakresu odpowiedzialności jego użytkowników i pracowników mających do niego dostęp.

§ 26 ust. 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.

Zakres tematyczny dokumentu procedur bezpiecznej eksploatacji

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.

Procedury bezpiecznej eksploatacji

Logo jednostki organizacyjnej	Nazwa /kryptonim Systemu TI	PBE
Tytuł / nazwa procedury		Nr / wersja Procedury:
Osoby realizujące:		
Nr rozdziału w dokumencie PBE:	Ilość stron:	Data wprowadzenia Procedury:	Data wycofania Procedury:

Sformalizowane podejścia do sposobu redagowania procedur bezpieczeństwa umożliwia m. in. skuteczne wprowadzanie zmian i uaktualnianie procedur bezpieczeństwa.

Zmiany w procedurach nie mogą być wprowadzane poprzez skreślenia lub poprawki.

Każda zmiana treści obowiązującej procedury wymaga napisania jej kolejnej wersji, która w całości zastępuje poprzednią i zaczyna obowiązywać od określonego terminu wskazanego w nagłówku procedury.

Procedury bezpiecznej eksploatacji

Logo jednostki organizacyjnej	Nazwa /kryptonim Systemu TI		PBE
Tytuł / nazwa procedury			Nr / wersja Procedury:
Osoby realizujące:			
Nr rozdziału w dokumencie PBE:	Ilość stron:	Data wprowadzenia Procedury:	Data wycofania Procedury:

Procedury bezpiecznej eksploatacji powinny zawierać wykaz czynności, poszczególnych użytkowników systemu TI wraz z dokładnym opisem sposobu ich wykonania.

Opisywane wykazy czynności powinny być pogrupowane w tematycznie wyodrębnione procedury.

Wszystkie procedury opracowane dla danego systemu powinny być spójne i opracowane według określonego schematu.

Treść procedur powinna być na tyle jasna i precyzyjna aby wszyscy użytkownicy po zapoznaniu się z ich treścią powinni jednoznacznie wiedzieć i rozumieć, jak realizować opisane w nich czynności.

Jeżeli treść procedur będzie zbyt skomplikowana lub zbyt ogólna może nie być odpowiednio realizowana.

Proces zarządzania ryzykiem

Proces zarządzania ryzykiem jest procesem ciągłym prowadzonym przez cały „cykl" przetwarzania informacji niejawnych w jednostce organizacyjnej, ze szczególnym uwzględnieniem informacji niejawnych przetwarzanych w systemach teleinformatycznych.

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.**

Najważniejszym zadaniem procesu zarządzania ryzykiem jest przedsięwzięcie świadomych i celowych działań ukierunkowanych na osiągniecie i utrzymanie zakładanego stopnia bezpieczeństwa przetwarzanych informacji niejawnych, który umożliwi redukcję i utrzymanie na poziomie akceptowanym przez kierownika jednostki organizacyjnej wielkości ryzyk związanych z ujawnieniem informacji niejawnych.

Proces zarządzania ryzykiem

Przed rozpoczęciem każdego procesu szacowania ryzyka należy:

1. **Ustalić granice i zakres analizy ryzyka.**
2. **Ustanowić strukturę organizacyjną odpowiedzialną za zarządzanie ryzykiem w systemie teleinformatycznym.**
3. **Dokonać wyboru metody analizy ryzyka.**

Szacowanie ryzyka dla bezpieczeństwa informacji niejawnych przetwarzanych w danym systemie teleinformatycznym jest procesem złożonym, na który składają się:

1. **analiza ryzyka,**

a. identyfikacja ryzyka,

- **zasoby systemu teleinformatycznego,**
- **zagrożenia,**
- **podatności,**
- **zabezpieczenia,**
- **skutki wystąpienia incydentu bezpieczeństwa teleinformatycznego;**

b. określenie wielkości ryzyk (wyznaczenie poziomów zidentyfikowanych ryzyk), ocena ryzyka (porównanie wyznaczonych poziomów ryzyk z tymi, które można zaakceptować).

2. **Ocena ryzyka (porównanie wyznaczonych poziomów ryzyk z tymi, które można zaakceptować).**

Proces zarządzania ryzykiem - określenie zbioru zagrożeń

Definiowanie szczegółowego zbioru potencjalnych przyczyn niepożądanych zdarzeń opiera się ściśle na zbiorze zasobów systemu, tzn. że **dla każdego z zasobów systemu należy indywidualnie zdefiniować zbiór potencjalnych przyczyn niepożądanych zdarzeń.**

Zbiór potencjalnych przyczyn zdarzeń niepożądanych zależy od rzeczywistych warunków funkcjonowania jednostki organizacyjnej i jako taki, nie jest regulowany ustawowo. Wyjątek stanowią **zagrożenia związane z ochroną elektromagnetyczną** oraz **ochroną kryptograficzną**, które w przypadku wykorzystywania ich w systemie obligatoryjnie muszą znaleźć się w zbiorze zagrożeń mogących wywołać szkody w zasobach systemu teleinformatycznego.

Zgodnie z § 2 pkt 15 rozporządzenia Prezesa Rady Ministrów z dnia 20 lipca 2011 r. w sprawie podstawowych wymagań bezpieczeństwa teleinformatycznego wyróżniamy siedem podstawowych kategorii zasobów systemu teleinformatycznego:

1. **Informacje przetwarzane w systemie teleinformatycznym.**
2. **Osoby.**
3. **Usługi.**
4. **Oprogramowanie.**
5. **Dane.**
6. **Sprzęt.**
7. **Inne elementy mające wpływ na bezpieczeństwo informacji przetwarzanych w systemie teleinformatycznych.**

Określenie zbioru zasobów systemu teleinformatycznego

Zbiór zasobów systemu powinien uwzględniać kategorie zasobów oraz odpowiadający im zbiór zagrożeń rozpatrywanych pod kątem atrybutów **poufności, integralności** i **dostępności**, przykładowo:

dla kategorii - **informacje przetwarzane w systemie teleinformatycznym**, biorąc pod uwagę zbiór potencjalnych zagrożeń (w tym przypadku ścisłe związany z atrakcyjnością przedmiotowych informacji) możemy wyodrębnić cztery zasoby systemu teleinformatycznego:

ZS-1 - informacje o klauzuli „zastrzeżone”,
ZS-2 - informacje o klauzuli „poufne”,
ZS-3 - informacje o klauzuli „tajne”,
ZS-4 - informacje o klauzuli „ściśle tajne”,

Określenie zbioru zasobów systemu teleinformatycznego

Zbiór zasobów systemu powinien uwzględniać kategorie zasobów oraz odpowiadający im zbiór zagrożeń rozpatrywanych pod kątem atrybutów **poufności, integralności** i **dostępności**, przykładowo:

dla kategorii – **osoby**, biorąc pod uwagę zbiór potencjalnych zagrożeń (przykładowo związany z poziomem wiedzy o systemie, zasadach jego działania, znajomością przepisów prawa czy stopień uprawnień w systemie) możemy wyodrębnić następujące zasoby systemu teleinformatycznego:

ZS-5 - kierownik jednostki organizacyjnej,

ZS-6 - pełnomocnik ds. ochrony informacji niejawnych,

ZS-7 - administrator systemu,

ZS-8 - inspektor bezpieczeństwa teleinformatycznego,

ZS-9 - użytkownicy,

Określenie zbioru zasobów systemu teleinformatycznego

Zbiór zasobów systemu powinien uwzględniać kategorie zasobów oraz odpowiadający im zbiór zagrożeń rozpatrywanych pod kątem atrybutów **poufności, integralności** i **dostępności**, przykładowo:

dla kategorii – **dane**, rozpatrując zbiór potencjalnych zagrożeń (w tym przypadku ścisłe związany z formą i postacią danych przetwarzanych i przechowywanych w systemie teleinformatycznym) możemy wyodrębnić następujące zasoby systemu teleinformatycznego:

ZS-10 - informacje niejawne utrwalone na kliszach,
ZS-11 - informacje niejawne utrwalone na mikrofilmach,
ZS-12 - informacje niejawne utrwalone na slajdach,
ZS-13 - informacje niejawne utrwalone na nośnikach optycznych,
ZS-14 - informacje niejawne utrwalone na nośnikach elektronicznych,
ZS-15 - informacje niejawne utrwalone na dyskach twardych wykorzystujących magnetyczne nośniki danych,

itd.

Szacowanie ryzyka

ZASOBY	SZACOWANIE	ZAGROŻENIA										
		POUFNOŚĆ				DOSTĘPNOŚĆ				INTEGRALNOŚĆ		
		ZG-1	ZG-2	ZG-5	ZG-6	ZG-1	ZG-2	ZG-4	ZG-8	ZG-1	ZG-3	ZG-7
ZS-1												
ZS-2												
ZS-3												
ZS-4												
ZS-n												

Proces zarządzania ryzykiem - Określenie wielkości przedziałów podatności

Określenie przedziałów prawdopodobieństwa (określanego w metodyce CRAM jako **podatność**) i przypisanie im zakresu wartości liczbowych jest warunkiem niezbędnym do przeprowadzenia procesu szacowania.

Poszczególnym zakresom podatności przypisuje się wartości liczbowe z przedziału od 0 do 10 (gdzie 0 oznacza brak podatności, natomiast 10 największą możliwą podatność danego zasobu systemu teleinformatycznego na dane zagrożenie).

Przykładowo dla poniższych pięciu przyjętych w jednostce organizacyjnej przedziałów podatność przypisano następujące wartości liczbowe z w/w przedziału:

Brak (0)
Niski poziom (1:3)
Średni poziom (4:6)
Podwyższony poziom (7:8)
Wysoki (9:10)

Zakresy oraz ilość przedziałów prawdopodobieństwa wystąpienia zdarzenia niepożądanego nie są regulowane przepisami prawa i zależą od indywidualnej decyzji osób przeprowadzających identyfikację ryzyka.

Proces zarządzania ryzykiem - Określenie wielkości przedziałów skutków wystąpienia incydentu bezpieczeństwa teleinformatycznego

Mimo wysiłku włożonego w zabezpieczenie informacji niejawnych niemożliwe jest całkowite wyeliminowanie zdarzeń niepożądanych w systemie teleinformatycznym.

Dlatego warunkiem niezbędnym dla prawidłowego przeprowadzenia szacowania ryzyka jest określenie wielkości konsekwencji ich wystąpienia (określanych w metodyce CRAM jako **skutki**) dla każdego z trzech podstawowych atrybutów systemu tj. **poufności, integralności** i **dostępności**.

Całej skali **skutków niepożądanych zdarzeń**, niezależnie od ich ilości, przypisuje się wartości liczbowe z przedziału od 1 do 10 (gdzie 1 oznacza minimalne skutki, natomiast 10 największy możliwy skutek).

O ile skala skutków wystąpienia incydentu bezpieczeństwa teleinformatycznego odnoszącego się do atrybutów dostępności i integralności zależy od osób przeprowadzających identyfikację ryzyka, o tyle skala skutków wystąpienia incydentu bezpieczeństwa teleinformatycznego odnoszącego się do atrybutu poufności uzależniona jest od klauzuli tajności poszczególnych zasobów systemu teleinformatycznego.

Przykładowo dla przyjętych w jednostce organizacyjnej skali skutków wystąpienia zdarzeń niepożądanych odnoszących się do atrybutów **dostępności** i **integralności** przypisano poniżej wartości liczbowe.

Proces zarządzania ryzykiem - Określenie wielkości przedziałów skutków wystąpienia incydentu bezpieczeństwa teleinformatycznego

Skutki wystąpienia incydentu bezpieczeństwa teleinformatycznego odnoszącego się do atrybutów dostępności i integralności oraz odpowiadające im wartości liczbowe:

Minimalne skutki (1:3)
Średnie skutki (4:6)
Poważne skutki (7:8)
Bardzo poważne skutki (9:10)

Skutki wystąpienia incydentu bezpieczeństwa teleinformatycznego odnoszącego się do atrybutów **poufności** i odpowiadające im wartości liczbowe:

Skutki ujawnienia informacji o klauzuli zastrzeżone (1:3)
Skutki ujawnienia informacji o klauzuli poufne (4:6)
Skutki ujawnienia informacji o klauzuli tajne (7:8)
Skutki ujawnienia informacji o klauzuli ściśle tajne (9:10)

Szacowanie ryzyka

ZASOBY	SZACOWANIE	ZAGROŻENIA										
		POUFNOŚĆ				DOSTĘPNOŚĆ				INTEGRALNOŚĆ		
		ZG-1	ZG-2	ZG-5	ZG-6	ZG-1	ZG-2	ZG-4	ZG-8	ZG-1	ZG-3	ZG-7
ZS-1	PODATNOŚĆ	3	5	3	4	3	3	3	5	2	3	5
	SKUTKI	3	3	3	3	2	2	2	2	3	3	3
ZS-2	PODATNOŚĆ	3	1	3	4	5	7	3	8	4	3	8
	SKUTKI	4	4	4	4	6	6	6	6	3	3	3
ZS-3	PODATNOŚĆ	9	3	4	8	5	5	5	5	9	9	9
	SKUTKI	5	5	5	5	3	3	3	3	4	4	4
ZS-4	PODATNOŚĆ	4	2	4	1	9	4	2	3	4	3	4
	SKUTKI	7	7	7	7	6	6	6	6	4	4	4
ZS-n	PODATNOŚĆ	4	2	3	3	5	3	7	3	4	3	1
	SKUTKI	6	6	6	6	3	3	3	3	2	2	2

Proces zarządzania ryzykiem - Określenie przedziałów wielkości ryzyk

W tym celu, analogicznie, jak to miało miejsce w przypadku określania podatności i skutków osoby przeprowadzające identyfikację ryzyka zobligowane są do określenia skali wielkości ryzyk przypisując im wartości liczbowe z przedziału od 0 do 100 (gdzie 0 oznacza brak ryzyka dla danego zagrożenia, natomiast 100 największą możliwą wartość ryzyka). Ryzyko to wyliczamy jako iloczyn podatności i skutków (R=PxS)

Przykładowo:

dla przyjętych w jednostce organizacyjnej skali wielkości ryzyk odnoszących się do atrybutu poufności, dostępności oraz integralności przypisano następujące wartości liczbowe:

Ryzyko niskie (0:20)

Ryzyko średnie (21:40)

Ryzyko podwyższone (41:60)

Ryzyko wysokie (61:80)

Ryzyko bardzo wysokie (80:100)

Następnie należy określić jaki poziom ryzyka jest akceptowalny (np. średni) i porównać go z ryzkiem wynikowym. Na podstawie tej oceny podejmuje się decyzję co do dalszego postępowania z ryzykami.

Szacowanie ryzyka

ZASOBY	SZACOWANIE	ZAGROŻENIA										
		POUFNOŚĆ				DOSTĘPNOŚĆ				INTEGRALNOŚĆ		
		ZG-1	ZG-2	ZG-5	ZG-6	ZG-1	ZG-2	ZG-4	ZG-8	ZG-1	ZG-3	ZG-7
ZS-1	PODATNOŚĆ	3	5	3	4	3	3	3	5	2	3	5
	SKUTKI	3	3	3	3	2	2	2	2	3	3	3
	RYZYKO	9	15	9	12	6	6	6	10	6	9	15
ZS-2	PODATNOŚĆ	3	1	3	4	5	7	3	8	4	3	8
	SKUTKI	4	4	4	4	6	6	6	6	3	3	3
	RYZYKO	12	4	12	16	30	42	18	48	12	9	24
ZS-3	PODATNOŚĆ	9	3	4	8	5	5	5	5	9	9	9
	SKUTKI	5	5	5	5	3	3	3	3	4	4	4
	RYZYKO	45	15	20	40	15	15	15	15	36	36	36
ZS-4	PODATNOŚĆ	4	2	4	1	9	4	2	3	4	3	4
	SKUTKI	7	7	7	7	6	6	6	6	4	4	4
	RYZYKO	28	14	28	7	54	24	12	18	16	12	16
ZS-n	PODATNOŚĆ	4	2	3	3	5	3	7	3	4	3	1
	SKUTKI	6	6	6	6	3	3	3	3	2	2	2
	RYZYKO	24	12	18	18	15	9	21	9	8	6	2

Podsumowanie

1. **Przetwarzanie informacji niejawnych tylko w akredytowanych systemach.**
   a. Opracowanie dokumentacji bezpieczeństwa.
   b. Przeprowadzenie oceny bezpieczeństwa systemu TI na podstawie dokumentacji bezpieczeństwa.
   c. Audyt bezpieczeństwa teleinformatycznego.
   d. Wydanie świadectwa akredytacji.
2. **Wyznaczenie osób funkcyjnych odpowiedzialnych za bezpieczeństwo systemu teleinformatycznego.**
   a. Powołanie administratora systemu.
   b. Powołanie inspektora bezpieczeństwa teleinformatycznego.
3. **Zarządzania ryzykiem.**
   a. Szacowania ryzyka dla bezpieczeństwa informacji niejawnych.
   b. Postępowania z ryzykiem.
   c. Akceptacji ryzyka.
   d. Przeglądu, monitorowania i informowania o ryzyku.
4. **Środki ochrony elektromagnetycznej.**
   a. Urządzenia o kontrolowanej emisji elektromagnetycznej (SDIP-27).
   b. Sprzętowa Strefa Ochrony Elektromagnetycznej.