

RAMOWY PLAN

warsztaty dla inspektorów, administratorów systemu i personelu bezpieczeństwa teleinformatycznego w tym – proces analizy i oceny ryzyka

Lp.	Czas	Temat	Prowadzący
1 dzień			
1.	09 ⁰⁰ – 09 ¹⁵	Otwarcie warsztatów, przedstawienie programu.	kmdr por. mgr inż. Marek Anzel Specjalista ds. ochrony informacji niejawnych i systemów teleinformatycznych
2.	09 ¹⁵ – 10 ⁰⁰	Prawne aspekty ochrony informacji w systemach teleinformatycznych. Ogólne zasady organizacji systemu TI. <ul style="list-style-type: none"> • Akty prawne normujące uruchomienie systemu TI • Zalecenia DBTI ABW / ZBIN SKW • Wytyczne szefa ABW w sprawie postępowania z informacjami niejawnymi międzynarodowymi 	-//-
3.	10 ⁰⁰ – 10 ⁴⁵	Bezpieczeństwo teleinformatyczne. Przebieg akredytacji systemu TI: <ul style="list-style-type: none"> • akredytacja systemów TI przeznaczonych do przetwarzania informacji niejawnych o klauzuli „poufne” i wyżej; • akredytacja systemów TI przeznaczonych do przetwarzania informacji niejawnych o klauzuli „zastrzeżone” • opłaty za postępowanie bezpieczeństwa TI 	-//-
4.	10 ⁴⁵ – 11 ⁴⁵	Bezpieczeństwo teleinformatyczne. Personel bezpieczeństwa TI <ul style="list-style-type: none"> • wyznaczenie osób funkcyjnych; • szkolenia specjalistyczne 	-//-
5.	11 ⁴⁵ – 13 ⁰⁰	Bezpieczeństwo fizyczne: <ul style="list-style-type: none"> • podstawowe kryteria i sposób określania poziomu zagrożeń; • dobór środków bezpieczeństwa fizycznego odpowiednich do wskazanego poziomu zagrożeń. 	-//-
6.	13 ⁰⁰ – 13 ³⁰	Przerwa kawowa	
7.	13 ³⁰ – 14 ⁴⁰	Bezpieczeństwo fizyczne - ĆWICZENIE: <ul style="list-style-type: none"> • metodyka doboru środków bezpieczeństwa fizycznego; • klasyfikacja środków bezpieczeństwa fizycznego. 	-//-
2 dzień			
1.	09 ⁰⁰ – 09 ³⁰	Ochrona Elektromagnetyczna: <ul style="list-style-type: none"> • wyznaczanie SSOE; • kategorie sprzętu TI ochrony E/mag Ochrona kryptograficzna	kmdr por. mgr inż. Marek Anzel
2.	09 ³⁰ – 10 ⁰⁰	Bezpieczeństwo osobowe - wymagania	-//-
3.	10 ⁰⁰ – 11 ⁴⁵	Kontrola dostępu: <ul style="list-style-type: none"> • warunki i sposób przydzielania użytkownikom uprawnień do pracy w systemie teleinformatycznym; • podstawowe zasady i procedury dotyczące hasel dostępu; • dziennik zdarzeń – logi systemowe – praktyczne przedstawienie przeglądania dziennika zdarzeń 	-//-
4.	11 ⁴⁵ – 13 ⁰⁰	Bezpieczeństwo teleinformatyczne. ETAPY: <ul style="list-style-type: none"> • etap planowania; • etap projektowania; • etap wdrażania; • etap eksploatacji; • etap wycofywania. 	-//-
5.	13 ⁰⁰ – 13 ³⁰	Przerwa kawowa	

6.	13 ³⁰ – 14 ⁴⁰	Zasady opracowania dokumentacji bezpieczeństwa. Opracowanie Szczególnych Wymagań Bezpieczeństwa (SWB) i Procedur Bezpiecznej Eksploatacji (PBE). Zakres obowiązków personelu bezpieczeństwa teleinformatycznego; <ul style="list-style-type: none"> • obowiązki kierownika jednostki organizacyjnej oraz pełnomocnika ochrony; • obowiązki IBTI oraz Administratora systemu. 	-//-
3 dzień			
1.	09 ⁰⁰ – 09 ⁴⁰	Bezpieczeństwo teleinformatyczne: <ul style="list-style-type: none"> • Systemy Zarządzania Bezpieczeństwem Informacji; • Normy ISO 27001 oraz 27005. 	kmdr por. mgr inż. Marek Anzel
2.	09 ⁴⁰ – 10 ³⁰	Bezpieczeństwo teleinformatyczne: <ul style="list-style-type: none"> • analiza ryzyka: wybór metody oraz etapy szacowania wartości informacji niejawnych i prawnie chronionych przetwarzanych w jednostce organizacyjnej. 	-//-
3.	10 ³⁰ – 10 ⁴⁵	Oznaczanie informatycznych nośników danych oraz sprzętu TI	
4.	10 ⁴⁵ – 11 ⁴⁰	Bezpieczeństwo teleinformatyczne - ĆWICZENIE:: <ul style="list-style-type: none"> • identyfikacja i szacowanie zasobów informacyjnych, identyfikacja zagrożeń i określenia ich poziomu, identyfikacja podatności na ryzyka. 	-//-
5.	11 ⁴⁰ – 13 ⁰⁰	Bezpieczeństwo teleinformatyczne - ĆWICZENIE:: <ul style="list-style-type: none"> • analiza i ocena ryzyka, dobór środków ochrony, akceptacja ryzyka szacunkowego. • utrzymanie złożonego poziomu bezpieczeństwa informacji, przegląd ryzyk i ocena skuteczności wprowadzonego poziomu zabezpieczeń. 	-//-
6.	13 ⁰⁰ – 13 ³⁰	Przerwa kawowa	
7.	13 ³⁰ – 14 ⁴⁰	Metryka dokumentu elektronicznego. Audyty. Testy bezpieczeństwa.	