

RAMOWY PLAN

Warsztatów dla: administratorów systemu i personelu bezpieczeństwa

PONIEDZIAŁEK		
09:00-10:30	Podstawowe wymagania i zadania w zakresie bezpieczeństwa teleinformatycznego informacji niejawnych. Zasady akredytacji systemów teleinformatycznych przeznaczonych do przetwarzania informacji niejawnych: - akty prawne normujące uruchomienie systemu teleinformatycznego; - proces akredytacji systemu TI („zastrzeżone” oraz „poufne” i wyżej); - bezpieczeństwo fizyczne; - bezpieczeństwo osobowe; - bezpieczeństwo elektromagnetyczne; - bezpieczeństwo kryptograficzne.	wykład
10:40-12:10	Dobór środków bezpieczeństwa fizycznego stosowanych do zabezpieczania pomieszczeń i obszarów, w których zorganizowano system TI: - Analiza Poziomu Zagrożeń; - Zakres stosowania środków bezpieczeństwa fizycznego w zależności od poziomu zagrożeń związanych z nieuprawnionym dostępem do informacji niejawnych lub ich utratą.	Ćwiczenia praktyczne
12:20-13:00	Zadania osób funkcyjnych w zakresie BTI: - kierownik jednostki organizacyjnej; - pełnomocnik ochrony; - IBTI; - administrator systemu.	wykład
13:00-13:20	Zasady nadawania uprawnień do dostępu do systemu TI	wykład
13:30-14:40	Zasady opracowania szczególnych wymagań bezpieczeństwa oraz procedur bezpiecznej eksploatacji	wykład
WTOREK		
09:00-09:45	Podstawowe zadania i obowiązki wynikające z rozporządzenia Prezesa Rady Ministrów z dnia 20 lipca 2011 r. w sprawie podstawowych wymagań bezpieczeństwa teleinformatycznego	Wykład
09:45-10:30	ETAPY funkcjonowania systemu teleinformatycznego	wykład
10:40-11:10	Ochrona informacji niejawnych pochodzących z wymiany międzynarodowej.	wykład
11:10-12:00	Dokumenty elektroniczne – metryki	wykład
12:10-13:00	Oznaczanie nośników i systemów TI	wykład
13:00-13:30	Kontrole z zakresu BTI. Organizacja, przeprowadzenie kontroli, dokumentowanie.	wykład
13:40-14:40	System Zarządzania Bezpieczeństwem Informacji.	wykład
ŚRODA		
09:00-09:40	Normy ISO stosowane w zarządzaniu ryzykiem.	
09:40-10:10	Analiza zagrożeń bezpieczeństwa informacji, szacowanie i zarządzanie ryzykiem, znaczenie ciągłości działania.	wykład
10:20-10:50	Wybrane metody szacowania ryzyka	wykład
11:00-14:25	Proces szacowania ryzyka dla bezpieczeństwa informacji niejawnych przetwarzanych w tym systemie.	Ćwiczenia praktyczne
14:25-14:40	Podsumowanie kursu. Odpowiedzi na pytania.	