Państwowa Wyższa Szkoła Zawodowa w Nysie

Instytut Bezpieczeństwa Wewnętrznego

Opis modułu kształcenia

Nazwa modułu (przedmiotu)	Zarządzanie bezpieczeństwem informacji	**Kod przedmiotu**	S-BW-I-P-BSI-ZBI_VI
Kierunek studiów	Bezpieczeństwo wewnętrzne		
Profil kształcenia	Praktyczny		
Poziom studiów	Studia pierwszego stopnia		
Specjalność	bezpieczeństwo systemów informatycznych, BSI		
Forma studiów	Studia stacjonarne		
Semestr studiów	VI		

					Zajęcia z zakresu nauk podstawowych				
Tryb zaliczenia przedmiotu		Egzamin		**Liczba punktów ECTS**					**Sposób ustalania oceny z przedmiotu**
Formy zajęć i inne	**L. godz. zajęć w sem.**			Całkowita	7	zajęcia kontaktowe	**2,4**	zajęcia praktyczne	**1,2**
	Całkowita	Pracy studenta	Kontaktowe	**Sposoby weryfikacji efektów kształcenia w ramach form zajęć**					Waga w %
Wykład	☐ 50	20	30	Test sprawdzajacy wiedzę					50%
Ćwiczenia praktyczne	☑ 125	95	30	Oceny cząstkowe z ćwiczeń					50%
	☐								
Razem:	***175***	***115***	***60***					Razem:	***100%***

Kategoria efektów	**L.p.**	**Efekty kształcenia dla modułu (przedmiotu)**	**Sposoby weryfikacji efektu kształcenia**	**Efekty kierunkowe**	**Efekty obszarowe**	**Uwagi**
Wiedza	1.	posiada podstawową wiedzę na temat zagrożeń systemów i sieci komputerowych	test wielokrotnego wyboru	K_W23++, K_W25++	T1P_W04++, T1P_W06++	
	2.	posiada wiedzę na temat podstawowych zabezpieczeń systemów i sieci komputerowych	test wielokrotnego wyboru	K_W25+++	T1P_W06+++	
	3.	Posiada wiedzę na temat zarządzania bezpieczeństem informacji w przedsiębiorstwie	test wielokrotnego wyboru	K_W25+++	T1P_W06+++	
Umiejętności	1.	Potrafi zaimplementować bezpieczny system komputerowy	Oceny z ćwiczeń	K_U14+++	T1P_U05+++	
	2.	Potrafi dbać o bezpieczeństwo danych, w tym o ich bezpieczne przesyłanie; posługuje się narzędziami kompresji i szyfrowania danych.	Oceny ćwiczeń	K_U13++	T1P_U04++	
	3.	Potrafi przeanalizować i wdrożyć procedury związane z zarządzaniem bezpieczeństwem informacji w skali przedsiębiorstwa	Oceny ćwiczeń	K_U13++, K_U14++	T1P_U04++, T1P_U05++	
Kompetencje społeczne	1.	Rozumie potrzebę ciągłego dokształcania się z zakresu zarządzania bezpieczeństwem informacji	Oceny ćwiczeń	K_K01++	S1P_K01++	
	2.	Rozumie potrzebę współdziałania przy realizacji projektów technicznych	Oceny ćwiczeń	K_K05++	T1P_K08++	
	3.					

Prowadzący

Forma zajęć	**Prowadzący zajęcia (tytuł/stopień naukowy, imię i nazwisko)**
Wykład	dr inż. Adam Sudoł
Ćwiczenia praktyczne	dr inż. Adam Sudoł

Treści kształcenia

Wykład	**Metody dydaktyczne**	Wykład / wykład problemowy / wykład z prezentacją multimedialną.

L.p.	**Tematyka zajęć**	**Liczba godzin**
1.	Wprowadzenie do tematyki bezpieczeństwa. Klasyfikacja zagrożeń w systemach i sieciach komputerowych, Motywy Ataków Podstawowe Usługi Zabezpieczające (usługi ochrony). Podstawowe Aspekty Zabezpieczenia Systemu i Sieci Komputerowej. Podstawy kryptografii.	4
2.	Rejestracja i uwierzytelnianie w systemach i sieciach komputerowych, podstawowe pojęcia, Infrastruktura klucza publicznego. Współczesne wykorzystanie PKI i systemu kerberos.	4
3.	Normy zarządzania bezpieczeństwem informacji. Podstawowe pojęcia i definicje zawarte w normie ISO/IEC 27001:2007.	4
4.	Podstawy polityki bezpieczeństwa informacji. Cel opracowywania i wdrażana PBI. Zakres merytoryczny PBI.	4
5.	Analiza i ocena ryzyka. Aktywa informacyjne i ich inwentaryzacja. Klasyfikacja informacji przetwarzanych przez organizację. Zagrożenia Podstawowa analiza kosztów i zysków.	4
6.	Zakres i Realizacja polityki bezpieczeństwa w następujących aspektach: Bezpieczeństwo zasobów ludzkich. Bezpieczeństwo fizycznym. Zarządzanie systemami i sieciami. Kontrola dostępu. Pozyskiwanie, rozwój i utrzymanie systemów informatycznych. Zarządzanie incydentami. Przygotowywanie planów ciągłości działania.	4
7.	Audytu wewnętrzny z zakresu PBI. Cele audytu. Wiedza i umiejętności audytora. Plan Audytu. Przeprowadzenie audytu. Zakończenie audytu – raport z audytu.	4
8.	Analiza przypadku.	2

Razem liczba godzin:	**30**

Ćwiczenia praktyczne	**Metody dydaktyczne**	

L.p.	**Tematyka zajęć**	**Liczba godzin**
1.	Wprowadzenie do tematyki bezpieczeństwa. Klasyfikacja zagrożeń w systemach i sieciach komputerowych, Motywy Ataków Podstawowe Usługi Zabezpieczające (usługi ochrony). Podstawowe Aspekty Zabezpieczenia Systemu i Sieci Komputerowej. Podstawy kryptografii.	8
2.	Rejestracja i uwierzytelnianie w systemach i sieciach komputerowych, podstawowe pojęcia, Infrastruktura klucza publicznego. Współczesne wykorzystanie PKI i systemu kerberos.	6
3.	Projekt polityki bezpieczeństwa dla wybranej firmy. : Na podstawie wytycznych podanych przez prowadzącego (potrzeby klienta) studenci będą opracowywać politykę bezpieczeństwa dla firmy. Rozwiązania te będą dyskutowane podczas zajęć z prowadzącym i pozostałymi studentami.	8
4.	Analiza przypadku: Na podstawie opracowań przygotowanych przez prowadzącego studenci będą analizować bezpieczeństwo wybranej firmy, zgodność zastosowanych rozwiązań z istniejącymi normami. Będą proponować własne rozwiązania. Studenci będą także przygotowywać dokumentacje niezbędną do przeprowadzania audytu teleinformatycznego.	8
	Razem liczba godzin:	**30**

Literatura podstawowa:

1	Monitoring i bezpieczeństwo sieci, Chris Fry, Martin Nystrom, Helion 2010
2	13 najpopularniejszych sieciowych ataków na Twój komputer. Wykrywanie, usuwanie skutków i zapobieganie, Maciej Szmit, Mariusz Tomaszewski, Dominika Lisiak, Izabela Politowska, Helion
3	Polityka bezpieczeństwa i ochrony informacji, Tadeusz Kifner, Helion1999

Literatura uzupełniająca:

1	żródła w internecie

…….. Koordynator modułu (przedmiotu)

podpis

……. Dyrektor Instytutu

pieczęć i podpis