Państwowa Wyższa Szkoła Zawodowa w Nysie

Instytut Bezpieczeństwa Wewnętrznego

Opis modułu kształcenia

Nazwa modułu (przedmiotu)	Zwalczanie przestępczości w cyberprzestrzeni	**Kod przedmiotu**	S-BW-I-P-BSI-ZPC_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		

Tryb zaliczenia przedmiotu	Egzamin	**Zajęcia z zakresu nauk podstawowych**					**Sposób ustalania oceny z przedmiotu**
Formy zajęć i inne	**L. godz. zajęć w sem.**	Całkowita	7	zajęcia kontaktowe	**1,8**	zajęcia praktyczne	**1,2**
	Całkowita / Pracy studenta / Kontaktowe	**Sposoby weryfikacji efektów kształcenia w ramach form zajęć**					Waga w %
Wykład	☐ 35 / 20 / 15	egzamin testowy					60%
Ćwiczenia praktyczne	☑ 140 / 110 / 30	ocena wykonania ćwiczeń					40%
	☐						
Razem:	***175 / 130 / 45***					Razem:	***100%***

Kategoria efektów	**L.p.**	**Efekty kształcenia dla modułu (przedmiotu)**	**Sposoby weryfikacji efektu kształcenia**	**Efekty kierunkowe**	**Efekty obszarowe**	**Uwagi**
Wiedza	1.	Ma podstawową wiedzę na temat zagrożeń jakie związane sa z rozwojem społeczeństwa informatycznego, ryzyka oraz metod zarządzania bezpieczeństwem w cyberprzestrzeni.	punkty za egzamin	K_W24++, K_W25+++	T1P_W05++, T1P_W06+++	
	2.	Ma podstawową wiedzę na temat norm i uwarunkowań prawnych polskich i międzynarodowych dotyczących cyberprzestępczości	punkty za egzamin	K_W24+++	T1P_W05+++	
	3.	ma podstawową wiedzę z zakresu wykrywania i dokumentowania incydentów oraz sposobów przeciwdziałania zagrożeniom	punkty za egzamin	K_W25+++	T1P_W06+++	
Umiejętności	1.	zna procedury dotyczące wykrywania i dokumentowania incydentów bezpieczeństwa	ocena z realizowanych ćwiczeń	K_U14+++	T1P_U05+++	
	2.	potrafi zastosować narzędzia wspomagające analizę incydentów, potrafi interpretować informacje z systemu komputerowego i systemów zabezpieczających.	ocena z realizowanych ćwiczeń	K_U13+++, K_U14++	T1P_U04+++, T1P_U05++	
Kompetencje społeczne	1.	Ma świadomość potrzeby ciągłego dokształcania i samodoskonalenia w zakresie wykonywanego zawodu oraz podnoszenia kompetencji zawodowych	ocena z realizowanych ćwiczeń	K_K01+	S1P_K01+	
	2.	Ma świadomość ważności profesjonalizmu działań podczas wykonywania czynności zawodowych	ocena z realizowanych ćwiczeń	K_K05++	T1P_K08++	
	3.					

Prowadzący

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

Treści kształcenia

Wykład	**Metody dydaktyczne**	wykład ilustrowany materiałami multimeedialnymi

L.p.	**Tematyka zajęć**	**Liczba godzin**
1.	społeczeństwo informatyczne. Tendencje rozwojowe technik i technologii i ich skutki społeczne.	1
2.	Polityka bezpieczeństwa. Zagrożenia i środki utrzymania bezpieczeństwa. Świadomość bezpieczeństwa. Kontrola dostępu. Bezpieczeństwo osobowe.	4
3.	Zagadnienia prawne. Normy w zakresie bezpieczeństwa teleinformatycznego. Czyny zabronione i regulacje zawarte w polskim prawie karnym. Rekomendacje, zalecenia i regulacje miedzynarodowe i obowiazujace w niektórych krajach.	3
4.	dopuszczalny zakres nadzoru i kontroli. Zapewnienie i poszanowania prywatności.	1
5.	Incydenty i sposoby ich dokumentowania. Procedury w zakresie postępowania w przypadku stwierdzenia zagrożeń i incydentów. Procedury w zakresie współpracy i wymiany informacji z instytucjami powołanymi do działań w zakresie cyberprzestępczości. Uzyskiwanie informacji na temat zagrożeń i podatności.	2
6.	metody przeciwdziałania zagrożeniom dla bezpieczeństwa danych i systemów.	2
7.	inżynieria społeczna i naruszenia norm związana z jej wykorzystaniem.	2
	Razem liczba godzin:	**15**

Ćwiczenia praktyczne	Metody dydaktyczne	ćwiczenia w labotarorium komputerowym

L.p.	Tematyka zajęć	Liczba godzin
1.	Zajęcia organizacyjne, przepisy BHP i regulamin pracowni komputerowej. Tematyka zajęć.	1
2.	logowanie informacji o zdarzeniach	2
3.	wykorzystanie narzędzi wspomagających analizę logów	3
4.	wykorzystanie narzedzi wykrywających anomalie w zachowaniu systemów do wykrywania ataków	4
5.	wykrycie prób nieautoryzowanego użycia systemu czy pozyskania danych z użyciem pułapki typu honeypot	4
6.	firewall'e. ids/ips, konfiguracja i analiza uzyskiwanych informacji	4
7.	analiza dostępnych w sieci czarnych list.	2
8.	przeciwdziałanie niektórym typom ataków	4
9.	analiza dostępnej informacji o zagrożeniach	2
10.	zaawansowane metody filtracji informacji	4
	Razem liczba godzin:	**30**

Literatura podstawowa:

1	Adamski A., Prawo karne komputerowe, Warszawa 2000,
2	Adamski A., Przestępczość w cyberprzestrzeni, Toruń 2001
3	N. Ferguson, B. Schneier, Kryptografia w praktyce., Helion, 2004
4	Lach A., Dowody elektroniczne w procesie karnym, Toruń 2004.
5	Goban-Klas T., Sienkiewicz P., Społeczeństwo informacyjne: szanse, zagrożenia, wyzwania, Kraków 1999.

Literatura uzupełniająca:

1	Liderman K.: Bezpieczeństwo teleinformatyczne, WSISiZ. Warszawa.2002
2	Stokłosa J., Ochrona danych w systemach komputerowych. Wyd. Politechniki Poznańskiej. Poznań 1997
3	Garfinkel S., Spafford G.: Bezpieczeństwo w Unixie i Internecie, Wydawnictwo RM. Warszawa. 1997

…….. ……

Koordynator modułu (przedmiotu) Dyrektor Instytutu

podpis pieczęć i podpis