POLITECHNIKA BYDGOSKA
Wydział Telekomunikacji, Informatyki i Elektrotechniki

Karta przedmiotu

Metody ochrony cyberprzestrzeni

1. Informacje podstawowe

Kierunek studiów informatyka stosowana	**Cykl kształcenia (nabór)** 2024/25
Specjalność systemy informatyczne	**Kod przedmiotu** 05ISTSIN.DI6D.0253.24
Jednostka zarządzająca kierunkiem studiów Wydział Telekomunikacji, Informatyki i Elektrotechniki	**Języki wykładowe** polski
Poziom studiów drugiego stopnia (mgr inż.)	**Obligatoryjność** Obligatoryjny specjalnościowy
Profil studiów Profil ogólnoakademicki	**Blok zajęciowy** Przedmioty specjalnościowe
Forma studiów studia niestacjonarne	

Wymagania wstępne	podstawy matematyki, zasady bezpieczeństwa
Przedmioty wprowadzające	matematyka
Koordynator	Jacek Majewski, Michał Choraś

Okres	**Forma i godziny zajęć**	**Liczba punktów ECTS**
Semestr 2	• Wykład: 18, Egzamin	2

Okres	**Forma i godziny zajęć**	**Liczba punktów ECTS**
Semestr 3	• Ćwiczenia laboratoryjne: 9, Zaliczenie na ocenę	2

2. Efekty uczenia się dla przedmiotu

Kod	Opis efektów uczenia się	Odniesienie do kierunkowych efektów uczenia się	Odniesienie do charakterystyk PRK
Wiedza:			
W1	ma rozszerzoną wiedzę na temat implementacji metod podnoszących bezpieczeństwo sieci teleinformatycznej	IST_O2_K_W12	P7S_WK P7S_WK_inż
W2	ma widzę z zakresu modelowania obiektów graficznych i ich identyfikacji w systemach podnoszących bezpieczeństwo	IST_O2_K_W14	P7S_WK P7S_WK_inż
W3	ma rozszerzoną i podbudowaną teoretycznie wiedzę w zakresie podstaw przetwarzania i przesyłania sygnałów zarówno lokalnie jak też w chmurze	IST_O2_K_W16	P7S_WK P7S_WK_inż
W4	orientuje się w obecnym stanie i najnowszych trendach rozwojowych informatyki	IST_O2_K_W17	P7S_WK P7S_WK_inż
W5	ma rozszerzoną wiedzę na temat modelowania procesów opisujących stan bezpieczeństwa sieci i systemu informatycznego	IST_O2_K_W19	P7S_WK P7S_WK_inż
Umiejętności:			
U1	Potrafi zaimplementować odpowiednie algorytmy przetwarzania sygnałów cyfrowych w celu podniesienia bezpieczeństwa systemu komputerowego	IST_O2_K_U12	P7S_UO
U2	potrafi dokonać wstępnej analizy ekonomicznej opracowanego projektu technicznego z zakresu ochrony danych	IST_O2_K_U15	P7S_UU
U3	potrafi analizować wybrane aspekty protokołów i usług w sieciach teleinformatycznych	IST_O2_K_U20	P7S_UU
Kompetencje społeczne:			
K1	ma świadomość roli społecznej absolwenta uczelni technicznej, rozumie potrzebę przekazywania społeczeństwu informacji dotyczących różnych aspektów informatyki w sposób jasny i zrozumiały	IST_O2_K_K05	P7S_KR

3. Treści programowe

Lp.	Treści programowe	Formy zajęć	Efekty uczenia się dla przedmiotu
1.	1. Ochrona infrastruktury krytycznej. 2. Metody zapewniania ciągłości usług. 3. Metody przeciwdziałania atakom skierowanym na bezpieczeństwo danych. 4. Metody zabezpieczania danych, zapewniających ich integralność. 5. Strategie i techniki obrony systemów informatycznych. 6. Normy i standardy bezpieczeństwa. 7. Zintegrowane systemy zabezpieczeń. 8. Strefy i monitorowanie bezpieczeństwa. 9. Wczesne wykrywanie i eliminowanie zagrożeń. 10. Zarządzanie bezpieczeństwem.	Wykład	W1, W2, W3, W4, W5

Lp.	Treści programowe	Formy zajęć	Efekty uczenia się dla przedmiotu
2.	Tematy projektów obejmują zagadnienia z zakresu omowianego obszaru W1, W2, W3, W4 i W5 efektów uczenia się realizowane dla MŚP.	Ćwiczenia laboratoryjne	U1, U2, U3, K1

4. Metody prowadzenia zajęć, weryfikacji efektów uczenia się i warunki zaliczenia

Semestr 2

Forma zajęć		
Wykład	**Metody prowadzenia zajęć:**	
	Wykład	
	Metody (sposoby) weryfikacji:	**Udział:**
	Zaliczenie pisemne	100%
	Warunki zaliczenia przedmiotu:	
	Uzyskanie z zaliczenia minimum 51% punktów stanowiących weryfikację uzyskanych (W1, W2, W3, W4, W5) efektów uczenia się.	

Semestr 3

Forma zajęć		
Ćwiczenia laboratoryjne	**Metody prowadzenia zajęć:**	
	Dyskusja, Projekt, Case study, Praca w grupie	
	Metody (sposoby) weryfikacji:	**Udział:**
	Projekt	70%
	Udział w dyskusji	20%
	Aktywność	10%
	Warunki zaliczenia przedmiotu:	
	Ocena projektu, rozwiązania postawionego problemu, aktywność w jego realizacji, planowość w realizacji etapów, współpraca w grupie, udział w dyskusji.	

Efekt uczenia się dla przedmiotu	**Metody (sposoby) weryfikacji**			
	Zaliczenie pisemne	Projekt	Aktywność	Udział w dyskusji
W1	x			
W2	x			
W3	x			
W4	x			

W5	x			
U1		x		x
U2		x		x
U3		x		x
K1		x	x	x

5. Literatura

Literatura podstawowa

1. Pipkin D. L., 2002, Bezpieczeństwo informacji. Ochrona globalnego przedsiębiorstwa, Wydawnictwo Naukowe PWN, Poznań 2002
2. Fry Ch, Nystrom M.,2010, Monitoring i bezpieczeństwo sieci, Helion
3. Krzysztof Liderman:Analiza ryzyka i ochrona informacji w systemach komputerowych, PWN, 2008

Literatura uzupełniająca

1. Viega J., 2010, Mity bezpieczeństwa IT. Czy na pewno nie masz się czego bać?, Helion,
2. Stokłosa J., Bilski T., Pankowski T., 2001, Bezpieczeństwo danych w systemach informatycznych, Wydawnictwo Naukowe PWN

6. Nakład pracy studenta - bilans godzin i punktów ECTS

Aktywność studenta		Obciążenie studenta Liczba godzin
Zajęcia prowadzone z bezpośrednim udziałem nauczyciela akademickiego lub innych osób prowadzących zajęcia	Wykład	18
	Ćwiczenia laboratoryjne	9
Praca własna studenta	Konsultacje	10
	Zbieranie informacji do zadanej pracy	10
	Przygotowanie do zajęć	35
	Przygotowanie projektu	20
Łączny nakład pracy studenta		102
Liczba punktów ECTS		4

* Godzina (dydaktyczna) oznacza 45 minut