POLITECHNIKA BYDGOSKA
Wydział Telekomunikacji, Informatyki i Elektrotechniki

Karta przedmiotu

Bezpieczeństwo internetu rzeczy

1. Informacje podstawowe

Kierunek studiów telekomunikacja i technologie internetu rzeczy	**Cykl kształcenia (nabór)** 2023/24
Specjalność -	**Kod przedmiotu** 05TTIRS.PI8C.1385.23
Jednostka zarządzająca kierunkiem studiów Wydział Telekomunikacji, Informatyki i Elektrotechniki	**Języki wykładowe** polski
Poziom studiów pierwszego stopnia (inż.)	**Obligatoryjność** Obowiązkowy
Profil studiów Profil ogólnoakademicki	**Blok zajęciowy** Przedmioty kierunkowe
Forma studiów studia stacjonarne	

Wymagania wstępne	Podstawowa znajomość konfiguracji oraz administrowania systemami operacyjnymi
Przedmioty wprowadzające	matematyka, podstawy elektroniki, podstawy telekomunikacji, sieci komputerowe, przemysłowy internet rzeczy (IIoT)
Koordynator	Jacek Majewski

Okres	**Forma i godziny zajęć**	**Liczba punktów ECTS**
Semestr 4	• Wykład: 15, Zaliczenie na ocenę • Ćwiczenia projektowe: 30, Zaliczenie na ocenę	3

2. Efekty uczenia się dla przedmiotu

Kod	**Opis efektów uczenia się**	**Odniesienie do kierunkowych efektów uczenia się**	**Odniesienie do charakterystyk PRK**
Wiedza:			

Kod	Opis efektów uczenia się	Odniesienie do kierunkowych efektów uczenia się	Odniesienie do charakterystyk PRK
W1	orientuje się w obecnym stanie bezpieczeństwa technologii, rozwiązań sieciowych oraz trendach rozwojowych systemów zabezpieczeń stosowanych w środowiskach internetu rzeczy	TTIR_O1_K_W08	P6S_WK
W2	ma uporządkowaną wiedzę dotyczącą bezpieczeństwa zasobów środowisk IoT w kontekście wymagań i norm i wpływu wykrywanych podatności na ewolucję stosowanych zabezpieczeń.	TTIR_O1_K_W08	P6S_WK
W3	posiada wiedzę w zakresie specyfiki środowisk IoT i jej wpływu na dobór stosowanych zabezpieczeń.	TTIR_O1_K_W08	P6S_WK
Umiejętności:			
U1	potrafi w sposób efektywny wskazać przydatność urządzenia lub technologii w działaniu podnoszącym bezpieczeństwo zasobów środowiska IoT.	TTIR_O1_K_U02	P6S_UW P6S_UW_inż
U2	posiada umiejętność dostosowania doboru środków podnoszących bezpieczeństwo z uwzględnieniem zmian wynikających z wykrytych podatności oraz ewolucji technologii	TTIR_O1_K_U08	P6S_UU
U3	potrafi dobrać odpowiednie mechanizmy ochrony przed zagrożeniami naruszenia atrybutów bezpieczeństwa informacji we wskazanym w zadaniu obszarze	TTIR_O1_K_U11	P6S_UW P6S_UW_inż
Kompetencje społeczne:			
K1	ma świadomość odpowiedzialności za realizowane zadania i wpływu na pracę zespołu	TTIR_O1_K_K03	P6S_KR
K2	potrafi w sposób zwięzły i jasny komunikować się, przestawiając zrealizowany zakres zadania wykorzystując w tym celu technologie informacyjne	TTIR_O1_K_K04	P6S_KO

3. Treści programowe

Lp.	Treści programowe	Formy zajęć	Efekty uczenia się dla przedmiotu
1.	1. Koncepcje bezpieczeństwa (poufność, integralność, dostępność, autentyczność i niezaprzeczalność). 2. Zagrożenia, ataki i aktywa – zależności i ich wpływ na bezpieczeństwo. 3. Podstawowe zasady projektowania bezpieczeństwa. 4. Ogólne zasady zarządzania bezpieczeństwem. 5. Standardy i normy bezpieczeństwa. 6. Kryptograficzna ochrona informacji środowiska internetu rzeczy. 7. Uwierzytelnianie użytkownika, urządzenia, oprogramowania w środowisku IoT. 8. Ochrona antywirusowa – rola infekcji w eskalacji cyberataku na infrastrukturę. 9. Model bezpieczeństwa „Zero Trust” dla środowisk IoT. 10. Specyfika bezpieczeństwa środowisk IoT – sieci przemysłowe IoT, infrastruktura ochrony zdrowia, smart city itd. 11. Bezpieczeństwo infrastruktury sieciowej. 12. Bezpieczeństwo w infrastrukturze chmury. W trakcie wykładu wybierane będą (jako przykłady do omówienia) aktualnie występujące incydenty z zakresu bezpieczeństwa.	Wykład	W1, W2, W3
2.	Tematami projektów realizowanymi w zespołach są zagadnienia obejmujące analizę wpływu wybranych technologii, metod oraz konfiguracji urządzeń wykorzystywanych w środowiskach IoT, wpływające na bezpieczeństwo funkcjonalne i ochronę przetwarzanej informacji.	Ćwiczenia projektowe	U1, U2, U3, K1, K2

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

Forma zajęć		
Wykład	**Metody prowadzenia zajęć:**	
	Wykład	
	Metody (sposoby) weryfikacji:	**Udział:**
	Test	100%
	Warunki zaliczenia przedmiotu:	
	Test (wielokrotnego wyboru z dodatnimi i ujemnymi punktami) zawiera zagadnienia z zakresu W1, W2 i W3 efektów uczenia się. Każdorazowo w przypadku zestawu pytań i odpowiedzi jest określana wartość minimalna punktów do uzyskania pozytywnej oceny (osiagnięcia powyżej 51 % efektów uczenia się). Pozostała skala ocen jest zgodna z: • poniżej 51% - niedostateczny (2,0) • od 51 % - dostateczny (3,0) • od 61 % - dostateczny plus (3,5) • od 71 % - dobry (4,0) • od 81 % - dobry plus (4,5) • od 91% - bardzo dobry (5,0)	

Ćwiczenia projektowe	**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**			
	Test	Projekt	Aktywność	Udział w dyskusji
W1	x			
W2	x			
W3	x			
U1		x		x
U2		x		x
U3		x		x
K1		x	x	x
K2		x	x	x

5. Literatura

Literatura podstawowa

1. J. Stokłosa, T. Bliski, T. Pankowski, „Bezpieczeństwo danych w systemach informatycznych”, PWN, 2001
2. J. Pieprzyk, T. Hardjono, J. Seberry, „Teoria bezpieczeństwa systemów komputerowych”, Helion, 2005
3. M. Liyanage, A. Braeken, P. Kumar, M. Ylianttila, “IoT Security: Advances in Authentication”, J. Wiley & Sons, 2019

Literatura uzupełniająca

1. W. R. Cheswick, „Firewalle i bezpieczeństwo w sieci” Helion, 2003
2. Akty prawne z obszaru bezpieczeństwa danych i cyberbezpieczeństwa.
3. Normy dotyczące bezpieczeństwa informacji ISO/IEC, PN
4. Raporty European Union Agency for Network and Information Security (https://www.enisa.europa.eu)

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	15
	Ćwiczenia projektowe	30
Praca własna studenta	Konsultacje	5
	Zbieranie informacji do zadanej pracy	5
	Przygotowanie do zajęć	10
	Przygotowanie projektu	20
Łączny nakład pracy studenta		85
Liczba punktów ECTS		3

* Godzina (dydaktyczna) oznacza 45 minut