Załącznik nr 9
do Zarządzenia Rektora PŚk Nr 35/19
w brzmieniu ustalonym Zarządzeniem Nr 12/22

KARTA PRZEDMIOTU

Kod przedmiotu	studia stacjonarne:	E-ID2C-05-s2, E-ID2C-05-s3
	studia niestacjonarne:	E-2IZ2C-1009-s3
Nazwa przedmiotu	**Bezpieczeństwo systemów IoT**	
Nazwa przedmiotu w języku angielskim	**Security of IoT Systems**	
Obowiązuje od roku akademickiego	**2022/23**	

USYTUOWANIE PRZEDMIOTU W SYSTEMIE STUDIÓW

Kierunek studiów	**Informatyka**
Poziom kształcenia	**II stopień**
Profil studiów	**Ogólnoakademicki**
Forma i tryb prowadzenia studiów	**Studia stacjonarne i niestacjonarne**
Zakres	**Cyberbezpieczeństwo**
Jednostka prowadząca przedmiot	**Katedra Systemów Informatycznych**
Koordynator przedmiotu	**Dr inż. Józef Ciosmak**
Zatwierdził	**Dziekan Wydziału Elektrotechniki, Automatyki i Informatyki dr hab. inż. Roman Deniziak, prof. PŚk**

OGÓLNA CHARAKTERYSTYKA PRZEDMIOTU

Przynależność do grupy/bloku przedmiotów		**Przedmiot specjalnościowy**
Status przedmiotu		**Wybieralny**
Język prowadzenia zajęć		**Polski**
Usytuowanie w planie studiów - semestr	studia stacjonarne	**Semestr II lub Semestr III**
	studia niestacjonarne	**Semestr II lub Semestr III**
Wymagania wstępne		**Wprowadzenie do cyberbezpieczeństwa, Społeczne aspekty cyberbezpieczeństwa.**
Egzamin (TAK/NIE)		**NIE**
Liczba punktów ECTS		**3**

Forma prowadzenia zajęć		**wykład**	**ćwiczenia**	**laborato-rium**	**projekt**	**inne**
Liczba godzin w semestrze	studia stacjonarne:	**30**			**30**	
	studia niestacjonarne:	**18**			**18**	

EFEKTY UCZENIA SIĘ

Kategoria	Symbol efektu	Efekty kształcenia	Odniesienie do efektów kierunkowych
Wiedza	W01	Student zna i rozumie współczesne problemy cyberbezpieczeństwa.	INF2_W02
	W02	Student dysponuje wiedzą pozwalającą na weryfikacją zabezpieczeń systemów IoT	INF2_W02
	W03	Student ma uporządkowaną wiedzę z zakresu architektury systemów IoT, organizacji i bezpieczeństwa.	INF2_W06
Umiejętności	U01	Student potrafi przeprowadzić czynności pozwalające ocenić stan zabezpieczenia systemu IoT i wskazać ewentualne braki.	INF2_U01, INF2_U02, INF2_U03, INF2_U05, INF2_U10
	U02	Student potrafi dobrać odpowiedni zestaw narzędzi programowych i sprzętowych dedykowanych dla systemów IoT w taki sposób, aby zapewnić wymagany poziom bezpieczeństwa.	INF2_U01, INF2_U05, INF2_U09 INF2_U10, INF2_U11
	U03	Student potrafi planować i przeprowadzać eksperymenty z zakresu ochrony informatycznej systemów IoT. Ponadto potrafi, przy użyciu odpowiednich metod i narzędzi, monitorować, wykrywać, usuwać i zapobiegać zagrożeniom.	INF2_U01, INF2_U03, INF2_U05, INF2_U07, INF2_U11
Kompetencje społeczne	K01	Student ma świadomość znaczenia cyberbezpieczeństwa w systemach IoT. Potrafi określić politykę bezpieczeństwa i zastosować rozwiązania informatyczne pozwalające ją zaimplementować.	INF2_K03, INF2_K04

TREŚCI PROGRAMOWE

Forma zajęć	Treści programowe
wykład	1.**Definicja Internetu Rzeczy (IoT)** (charakterystyka, wymagania i cele stawiane IoT). 2.**Architektury systemów IoT**(przykłady rozwiązań od prostych implementacji po rozbudowane systemy sprzętowe i programowe. Ograniczenia konstrukcyjne i funkcjonalne). 3.**Wymiana informacji w systemach IoT**(interfejsy komunikacyjne, standardy komunikacji przewodowej i bezprzewodowej, kryteria doboru komunikacji w zależności od warunków środowiskowych i wymaganego bezpieczeństwa transmisji). 4. **Bezpieczeństwo w systemach IoT** (wymagania, podatność wybranych komponentów – analiza przykładów, identyfikacja, uwierzytelnianie). 5.**Prawa dostępu w sieciach IoT**(wymagania w projektowaniu zabezpieczeń, wybór typów i rodzajów zabezpieczeń, analiza poziomu zabezpieczeń). 6.**Bezpieczeństwo aplikacji** (bezpieczeństwo dedykowanego oprogramowania dla systemów IoT, środowiska uruchomieniowe, środowiska systemowe, zabezpieczenia tworzonych aplikacji dla IoT, narzędzia zabezpieczające). 7.**Zabezpieczenia urządzeń IoT w sieciach** (usługi sieciowe, obciążenia sieci danymi z wielu modułów IoT, separacja sieci, wykrywanie potencjalnych wycieków danych i włamań, szyfrowanie danych). 8.**Zarządzanie systemami IoT** (pod kątem bezpieczeństwa użytkowania i ochrony danych wrażliwych, ustawianie poziomu zabezpieczeń).

projekt	1. Studium wybranych narzędzi programistycznych i sprzętowych wykorzystywanych w systemach IoT. 2. Wykonanie zadania projektowego z zakresu bezpieczeństwa wybranego podsystemu IoT – analiza komponentów, analiza oprogramowania, ocena platformy wymiany danych, monitorowanie zdarzeń, testy bezpieczeństwa.

METODY WERYFIKACJI EFEKTÓW UCZENIA SIĘ

Symbol efektu	Metody sprawdzania efektów kształcenia					
	Egzamin ustny	Egzamin pisemny	Kolokwium	Projekt	Sprawozdanie	Inne
W01			X			
W02			X			
W03			X			
U01				X		
U02				X		
U03				X		
K01				X		

FORMA I WARUNKI ZALICZENIA

Forma zajęć	Forma zaliczenia	Warunki zaliczenia
wykład	zaliczenie z oceną	Uzyskanie co najmniej 50% punktów z kolokwium.
projekt	zaliczenie z oceną	Uzyskanie co najmniej 50% punktów z zadań projektowych.

NAKŁAD PRACY STUDENTA

Bilans punktów ECTS													
Lp.	Rodzaj aktywności	Obciążenie studenta										Jednostka
		studia stacjonarne					studia niestacjonarne					
1.	Udział w zajęciach zgodnie z planem studiów	W	C	L	P	S	W	C	L	P	S	h
		30			30		18			18		
2.	Inne (konsultacje, egzamin)	2			2		2			2		h
3.	**Razem przy bezpośrednim udziale nauczyciela akademickiego**	**64**					**40**					h
4.	**Liczba punktów ECTS, którą student uzyskuje przy bezpośrednim udziale nauczyciela akademickiego**	**2,56**					**1,6**					ECTS
5.	**Liczba godzin samodzielnej pracy studenta**	**11**					**35**					h
6.	**Liczba punktów ECTS, którą student uzyskuje w ramach samodzielnej pracy**	**0,44**					**1,4**					ECTS
7.	**Nakład pracy związany z zajęciami o charakterze praktycznym**	**30**					**18**					h

8.	**Liczba punktów ECTS, którą student uzyskuje w ramach zajęć o charakterze praktycznym**	**1,2**	**0,72**	ECTS
9.	**Sumaryczne obciążenie pracą studenta**	**75**	**75**	h
10.	**Punkty ECTS za moduł** *1 punkt ECTS=25 godzin obciążenia studenta*	**3**		ECTS

LITERATURA

1. Wojciech Mielczarek, „Szeregowe interfejsy cyfrowe", Helion 2011, ISBN: 83-857-0123-0, 8385701230.
2. Madhusanka Liyanage; An Braeken; Pardeep Kumar; Mika Ylianttila, „IoT Security: Advances in Authentication", Wiley 2020, ISBN: 9781119527923.
3. Marcin Sikorski, „ Internet rzeczy", PWN 2020, ISBN:9788301208400.
4. Jerzy Krawiec, „ Internet Rzeczy (IoT). Problemy cyberbezpieczeństwa", eBook, 2020, ISBN:978-83-8156-438-0, ISBN druku:978-83-8156-108-2.
5. Michał Mostowik, „Ochrona danych osobowych w Internecie Rzeczy w prawie UE", C.H.Beck 2022, ISBN:978-83-8235-882-7 ISBN druku:978-83-8235-881-0.