

KARTA PRZEDMIOTU

Nazwa w języku polskim: **Bezpieczeństwo systemów IoT**

Nazwa w języku angielskim: **Security of IoT systems**

Karta przedmiotu ważna od roku akademickiego: **2022/2023**

Kierunek studiów: **Informatyka**

Poziom studiów: **Studia I stopnia**

Forma studiów: **Niestacjonarne**

Profil: **Praktyczny**

Specjalność: **Cyberbezpieczeństwo**

Język wykładowy: **Polski**

Jednostka prowadząca: **Wydział Nauk Społecznych i Technicznych**

Prowadzący: **dr inż. Zdzisław Pólkowski, prof. UJW**

OBCIĄŻENIE STUDENTA

	Wykład	Konwersatorium	Laboratorium	Projekt	Seminarium
Liczba godzin zajęć dydaktycznych organizowanych przez Uczelnię	10				
Liczba godzin całkowitego nakładu pracy studenta	50				
Forma zaliczenia	Zaliczenie z oceną				
Liczba punktów ECTS	2				

WYMAGANIA WSTĘPNE W ZAKRESIE WIEDZY, UMIEJĘTNOŚCI I INNYCH KOMPETENCJI

Podstawowa znajomość zagadnień z zakresu bezpieczeństwa informacyjnego i informatycznego.

CELE PRZEDMIOTU

C1	Nabywanie przez studentów wszechstronnej wiedzy oraz umiejętności z zakresu bezpieczeństwa IoT.
C2	Nabywanie wiedzy oraz umiejętności w kwestii określenia podstawowych zagrożeń bezpieczeństwa IoT.
C3	Zapoznanie studentów z nowymi zagrożeniami związanymi z działaniem systemów gromadzenia, monitorowania i transmisji danych w systemach IoT.

PRZEDMIOTOWE EFEKTY UCZENIA – PEU	
Z zakresu wiedzy:	
PEU_W01	Posiada wiedzę dotyczącą terminologii i dylematów bezpieczeństwa systemów IoT.
PEU_W02	Posiada wiedzę dotyczącą zagrożeń systemów IoT.
Z zakresu umiejętności:	
PEU_U01	Potrafi analizować przypadki zagrożeń systemów IoT, oraz wskazuje skuteczne metody zapewnienia bezpieczeństwa systemów IoT.
Z zakresu kompetencji społecznych:	
PEU_K01	Jest świadomy roli edukacji w zakresie bezpieczeństwa systemów IoT, jest gotów rozwijać swoją wiedzę i edukować.

TREŚCI PROGRAMOWE		
Forma zajęć – wykład		Liczba godzin
W1	Omówienie zasad zaliczenia przedmiotu. Wprowadzenie dotyczące bezpieczeństwa informacyjnego i informatycznego systemów IoT.	1
W2	Idea koncepcji Internetu rzeczy.	1
W3	Rodzaje podatności systemów IoT	1
W4	Potencjalne zagrożenia systemów IoT.	1
W5	Sposoby zabezpieczeń systemów IoT.	1
W6	Protokoły komunikacji oraz rozproszonych systemów obliczeniowych: Cloud, Edge oraz Fog Computing wykorzystywanych w systemach IoT.	1
W7	Wykorzystanie technologii Blockchain w celu zapewnienia bezpieczeństwa systemów IoT.	1
W8	Wykorzystanie Artificial Intelligence w celu zapewnienia bezpieczeństwa systemów IoT.	1
W9	Wykorzystanie Machine Learning w celu zapewnienia bezpieczeństwa systemów IoT. Przykłady ataków na systemy IoT.	1
W10	Podsumowanie, zaliczenie.	1
Razem		10

STOSOWANE NARZĘDZIA DYDAKTYCZNE	
1.	Prezentacja treści z wykorzystaniem multimedialnych.
2.	Sprawozdanie w formie cyfrowej z wykonanych zadań.
3.	Miniprojekt zawierający analizę wybranego zagadnienia wraz z obliczeniami wykonanymi metodami

	komputerowymi.
4.	Esej dotyczący aktualnych trendów w obszarze informatyki w zarządzaniu.

METODY I FORMY OCENY
OSIĄGNIĘCIA PRZEDMIOTOWYCH EFEKTÓW UCZENIA

Formy oceny (F lub P)*	Numer efektu uczenia (przedmiotowego)	Metody oceny osiągnięcia efektu uczenia
F w	PEU_W01, PEU_W02, PEU_U01	Prezentacja. Sprawozdanie, esej.
P w	PEU_W01, PEU_W02, PEU_U01 PEU_K01	Zaliczenie w formie ustnej i/lub pisemnej.

*F – ocena formująca (w trakcie semestru), P – ocena podsumowująca (na koniec semestru)

KRYTERIA OCENY
OSIĄGNIĘCIA PRZEDMIOTOWYCH EFEKTÓW UCZENIA

Nr PEU	Ocena dostateczna	Ocena dobra	Ocena bardzo dobra
PEU_W01	Posiada podstawową wiedzę dotyczącą terminologii i dylematów bezpieczeństwa systemów IoT.	Posiada pogłębioną wiedzę dotyczącą terminologii i dylematów bezpieczeństwa systemów IoT.	Posiada szczegółową wiedzę dotyczącą terminologii i dylematów bezpieczeństwa systemów IoT.
PEU_W02	Posiada podstawową wiedzę dotyczącą zagrożeń systemów IoT.	Posiada pogłębioną wiedzę dotyczącą zagrożeń systemów IoT.	Posiada szczegółową wiedzę dotyczącą zagrożeń systemów IoT.
PEU_U01	Z pomocą wykładowcy analizuje nieskomplikowane przypadki zagrożeń systemów IoT, oraz wskazuje skuteczne metody zapewnienia bezpieczeństwa systemów IoT.	Definiuje, porównuje, analizuje przypadki zagrożeń systemów IoT, oraz wskazuje skuteczne metody zapewnienia bezpieczeństwa systemów IoT.	Samodzielnie definiuje, porównuje, analizuje skomplikowane przypadki zagrożeń systemów IoT oraz wskazuje skuteczne metody zapewnienia bezpieczeństwa systemów IoT.
PEU_K01	Jest świadomy roli edukacji w zakresie bezpieczeństwa systemów IoT.	Jest w pełni świadomy roli edukacji w zakresie bezpieczeństwa systemów IoT. Jest gotów rozwijać swoją wiedzę.	Jest w pełni świadomy roli edukacji w zakresie bezpieczeństwa systemów IoT, samodzielnie edukuje w tym zakresie oraz poszerza własną wiedzę.

LITERATURA PODSTAWOWA

Internet Rzeczy (IoT). Problemy cyberbezpieczeństwa, Jerzy Krawiec, Oficyna Wydawnicza Politechniki Warszawskiej.

LITERATURA UZUPEŁNIAJĄCA

F. Chantzis, I. Stais, P. Calderon, Hakowanie internetu rzeczy w praktyce. Przewodnik po skutecznych metodach atakowania IoT., Evangelos Deirmentzoglou i in., Helion.

Internet of Things (IoT) Security, Sharad Agarwal, [Online]
https://cds.cern.ch/record/2776796/files/report_sharad_argawal.pdf, dostęp 28.11.2022.

ŹRÓDŁA ELEKTRONICZNE

Portal edukacyjny dra inż. Zdzisława Półkowskiego, prof. UJW www.moodle.polkowski.edu.pl

Cyberbezpieczeństwo w Polsce w 2021 r, cyberataki na urządzenia końcowe, [Online] https://cyfrowapolska.org/wp-content/uploads/2022/01/Cyfrowa_Polska-Raport_Cyberzagrozenia2021.pdf, dostęp 25.11.2022.

Cyberbezpieczeństwo, [Online] https://codozasady.pl/upload/wordpress/2014/12/raport_cyberbezpieczenstwo.pdf, dostęp 27.11.2022.

[Online] <https://www.netacad.com/courses/iot>, dostęp 27.11.2022.

MACIERZ POWIĄZANIA

EFEKTÓW UCZENIA DLA PRZEDMIOTU BEZPIECZEŃSTWO SYSTEMÓW IOT Z EFEKTAMI UCZENIA NA KIERUNKU INFORMATYKA

Przedmiotowy efekt uczenia	Odniesienie przedmiotowego efektu do efektów uczenia zdefiniowanych dla kierunku studiów i specjalności	Cele przedmiotu	Treści programowe	Numer narzędzia dydaktycznego
PEU_W01	K_W01, K_W02	C1, C2	W1, W2, W3, W4, W5, W6, W7, W8, W9, W10,	1, 2, 2, 4
PEU_W02	K_W03, K_W08	C1, C2	W1, W2, W3, W3, W4, W5, W6, W7, W8, W9, W10,	1, 2, 3, 4
PEU_U01	K_U01, K_U02, K_U07	C2, C3	W6, W7, W8, W9, W10,	1, 2, 3, 4
PEU_K01	K_K01, K_K02, K_K04	C2, C3	W3, W4, W6	1, 2, 3,4