

KARTA PRZEDMIOTU

Nazwa w języku polskim: **Podstawy cyberbezpieczeństwa**

Nazwa w języku angielskim: **Cybersecurity basics**

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	26				
Liczba godzin całkowitego nakładu pracy studenta	100				
Forma zaliczenia	Egzamin				
Liczba punktów ECTS	4				

WYMAGANIA WSTĘPNE W ZAKRESIE WIEDZY, UMIEJĘTNOŚCI I INNYCH KOMPETENCJI

Podstawowa znajomość zagadnień z zakresu bezpieczeństwa informacyjnego i informatycznego.

CELE PRZEDMIOTU

C1	Nabycie przez studentów wszechstronnej wiedzy oraz umiejętności z zakresu cyberbezpieczeństwa, w szczególności krajowego i unijnego systemu cyberbezpieczeństwa usług kluczowych i usług cyfrowych.
C2	Nabycie wiedzy oraz umiejętności w kwestii określenia podstawowych zagrożeń cyberbezpieczeństwa (incydentów sieciowych), zadań operatorów usług kluczowych i dostawców usług cyfrowych.
C3	Zapoznanie studentów z nowymi zagrożeniami związanymi z działaniem systemów gromadzenia, monitorowania i transmisji danych w cyberprzestrzeni.

PRZEDMIOTOWE EFEKTY UCZENIA – PEU	
Z zakresu wiedzy:	
PEU_W01	Posiada wiedzę dotyczącą terminologii i dylematów cyberbezpieczeństwa.
PEU_W02	Posiada wiedzę dotyczącą zagrożeń systemów gromadzenia i transmisji danych w cyberprzestrzeni.
Z zakresu umiejętności:	
PEU_U01	Potrafi porównywać i analizować przypadki cyberzagrożeń, omawia skuteczne metody zapewnienia bezpieczeństwa systemów komputerowych.
Z zakresu kompetencji społecznych:	
PEU_K01	Jest świadomy roli edukacji w zakresie cyberbezpieczeństwa.

TREŚCI PROGRAMOWE		
Forma zajęć – wykład		Liczba godzin
W1	Wprowadzenie, omówienie zasad zaliczenia przedmiotu. Cyberprzestępczość, cyberbezpieczeństwo oraz cyberprzestrzeń – wprowadzenie.	2
W2	Cyberbezpieczeństwo przetwarzania danych osobowych, RODO.	2
W3	Krajowy system cyberbezpieczeństwa, KRI.	2
W4	Cyberterroryzm, cyberwojna.	1
W5	Instytucje zwalczające cyberzagrożenia.	1
W6	Zagrożenia w cyfrowej rzeczywistości, rodzaje ataków, sposoby wykrywania i reagowania.	2
W7	Złośliwe oprogramowanie - sposoby ochrony.	2
W8	Kontrola dostępu i metody szyfrowania. Kryptografia symetryczna vs kryptografia asymetryczna.	2
W9	Metody ataków na usługi sieciowe oraz infrastrukturę. Bezpieczeństwo protokołów wykorzystywanych w sieciach lokalnych i bezprzewodowych.	2
W10	Systemy szyfrowania, uwierzytelniania oraz infrastruktura klucza publicznego w sieciach VPN.	2
W11	Zapobieganie wyciekom danych, analiza powłamaniowa i ukrywanie ataków.	2
W12	Systemy wykrywania intruzów oraz wykrywania ataków.	2
W13	Polityka bezpieczeństwa systemów informatycznych oraz metodyka projektowania zabezpieczeń.	2
W14	Podsumowanie. Zaliczenie przedmiotu.	2
Razem		26

STOSOWANE NARZĘDZIA DYDAKTYCZNE

1.	Prezentacja treści z wykorzystaniem multimediiów.
2.	Sprawozdanie w formie cyfrowej z wykonanych zadań.
3.	Miniprojekt zawierający analizę wybranego zagadnienia wraz z obliczenia 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
Fw	PEU_W01, PEU_W02, PEU_U01, PEU_K01	Prezentacja. Sprawozdanie, esej.
Pw	PEU_W01, PEU_W02, PEU_U01, PEU_K01	Egzamin w formie ustnej 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 cyberbezpieczeństwa.	Posiada pogłębianą wiedzę dotyczącą terminologii i dylematów cyberbezpieczeństwa.	Posiada szczegółową wiedzę dotyczącą terminologii i dylematów cyberbezpieczeństwa.
PEU_W02	Posiada podstawową wiedzę dotyczącą zagrożeń systemów gromadzenia i transmisji danych w cyberprzestrzeni.	Posiada pogłębianą wiedzę dotyczącą zagrożeń systemów gromadzenia i transmisji danych w cyberprzestrzeni.	Posiada szczegółową wiedzę dotyczącą zagrożeń systemów gromadzenia i transmisji danych w cyberprzestrzeni.
PEU_U01	Potrafi definiować, porównuje i analizuje tylko wybrane przypadki cyberzagrożeń, wskazuje skuteczne metody zapewnienia bezpieczeństwa systemów komputerowych.	Potrafi definiować, porównuje i analizuje przypadki cyberzagrożeń, wskazuje skuteczne metody zapewnienia bezpieczeństwa systemów komputerowych.	Potrafi definiować, porównuje i analizuje skomplikowane przypadki cyberzagrożeń, wskazuje skuteczne metody zapewnienia bezpieczeństwa systemów komputerowych.
PEU_K01	Jest świadomy roli edukacji w zakresie cyberbezpieczeństwa.	Jest w pełni świadomy roli edukacji w zakresie cyberbezpieczeństwa.	Jest w pełni świadomy roli edukacji w zakresie cyberbezpieczeństwa, potrafi samodzielnie edukować w zakresie cyberbezpieczeństwa.

LITERATURA PODSTAWOWA

Wprowadzenie do bezpieczeństwa IT, praca zbiorowa, Wyd. Securitum, 2023.

M. Szmit, M. Gusta, M. Tomaszewski, 101 zabezpieczeń przed atakami w sieci komputerowej, Helion 2005.

W. Stallings, Kryptografia i bezpieczeństwo sieci komputerowych. Matematyka szyfrów i techniki kryptografii, Helion 2011. Helion 2009.

LITERATURA UZUPEŁNIAJĄCA

M. Serefin, Sieci VPN. Praca zdalna i bezpieczeństwo danych, wyd. II rozszerzone,

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

MACIERZ POWIĄZANIA

EFEKTÓW UCZENIA DLA PRZEDMIOTU PODSTAWY CYBERBEZPIECZEŃSTWA

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, W3, W4, W5, W6, W7, W8, W9, W10, W11, W12, W13, W14	1, 2, 4
PEU_W02	K_W03, K_W08	C1, C2	W1, W2, W3, W3, W4, W5, W6, W7, W8, W9, W10, W11, W12, W13, W14	1, 2, 4
PEU_U01	K_U01, K_U02, K_U04, K_U05 K_U08	C2, C3	W6, W7, W8, W9, W10, W11, W12	1, 2, 4
PEU_K01	K_K01, K_K02, K_K04	C2, C3	W3, W4, W6	1, 2, 3,4