

KARTA PRZEDMIOTU

Nazwa w języku polskim: **Podstawy cyberbezpieczeństwa**

Nazwa w języku angielskim: **Basics of Cybersecurity**

Karta przedmiotu ważna od roku akademickiego: **2026/2027**

Kierunek studiów: **Zarządzanie**

Poziom studiów: **Studia I stopnia**

Forma studiów: **Niestacjonarne**

Profil: **Praktyczny**

Specjalność: **E-commerce**

Język wykładowy: **Polski**

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

Opiekun przedmiotu: **dr Jolanta Dmowska, prof. UJW**

OBCIĄŻENIE STUDENTA

	Konwersatorium	Ćwiczenia	Laboratorium	Projekt	Seminarium
Liczba godzin zajęć dydaktycznych organizowanych przez Uczelnię	10				
Liczba godzin całkowitego nakładu pracy studenta	50				
Forma zaliczenia	zaliczenie na ocenę				
Liczba punktów ECTS	2				

WYMAGANIA WSTĘPNE W ZAKRESIE WIEDZY, UMIEJĘTNOŚCI I INNYCH KOMPETENCJI

Brak

CELE PRZEDMIOTU

C1	Celem przedmiotu jest nabycie wiedzy nt. podstawowych zagadnień związanych z cyberbezpieczeństwem, w szczególności zagadnień dotyczących ochrony informacji i zasobów e-organizacji wobec zagrożeń cyfrowych
C2	Zdobycie umiejętności identyfikacji zagrożeń cyfrowych oraz reagowania na incydenty w e-organizacji

PRZEDMIOTOWE EFEKTY UCZENIA – PEU

Z zakresu wiedzy:

PEU_W01	Posiada zaawansowaną wiedzę na temat regulacji prawnych dot. cyberbezpieczeństwa
----------------	--

PEU_W02	Posiada zaawansowaną wiedzę z zakresu zagrożeń cyfrowych - bezpiecznego przechowywania danych
Z zakresu umiejętności:	
PEU_U01	Potrafi zidentyfikować zagrożenia cyfrowe w organizacjach
Z zakresu kompetencji społecznych:	
PEU_K01	Potrafi współdziałać i pracować w grupie, przyjmując w niej różne role, zgodnie z zasadami etyki zawodowej

TREŚCI PROGRAMOWE		
Forma zajęć – Konwersatorium		Liczba godzin
K1	Wprowadzenie. Przegląd regulacji prawnych dot. cyberbezpieczeństwa	2
K2	Przegląd zagrożeń cyfrowych w e-organizacjach. Bezpieczne przechowywanie danych	
K3	Praktyki w zarządzaniu hasłami i uwierzytelnieniem	
K4	Analiza przypadków rzeczywistych ataków hakerskich	
K5	Zaliczenie przedmiotu	2
Razem		10

STOSOWANE NARZĘDZIA DYDAKTYCZNE	
1.	Konwersatorium: – metoda tradycyjna z wykorzystaniem multimediów – dyskusja moderowana – analiza przypadków (case studies) – praca w grupie – debata oksfordzka

METODY I FORMY OCENY

OSIĄGNIĘCIA PRZEDMIOTOWYCH EFEKTÓW UCZENIA

Formy oceny (F lub P)*	Numer efektu uczenia (przedmiotowego)	Metody oceny osiągnięcia efektu uczenia
P	PEU_W01, PEU_W02, PEU_U01	Zaliczenie pisemne
F	PEU_W01, PEU_W02, PEU_U01, PEU_K01	Ocena zaangażowania na zajęciach

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

KRYTERIA OCENY

OSIĄGNIĘCIA PRZEDMIOTOWYCH EFEKTÓW UCZENIA

Nr PEK	Ocena dostateczna	Ocena dobra	Ocena bardzo dobra
PEU_W01	Student potrafi wymienić podstawowe regulacje prawne dot. cyberbezpieczeństwa	Student potrafi wymienić i omówić podstawowe regulacje prawne dot. cyberbezpieczeństwa	Student potrafi wymienić i omówić podstawowe regulacje prawne dot. cyberbezpieczeństwa oraz podać przykłady zastosowania tych regulacji w e-organizacji
PEU_W02	Student potrafi wymienić i omówić rodzaje zagrożeń cyfrowych	Student potrafi wymienić i omówić rodzaje zagrożeń cyfrowych oraz adekwatne zasady bezpiecznego przechowywania danych	Student potrafi wymienić i omówić rodzaje zagrożeń cyfrowych oraz adekwatne zasady bezpiecznego przechowywania danych podać przykłady ich zastosowania w e-organizacji
PEU_U01	Student potrafi zidentyfikować rodzaje zagrożeń cyfrowych na wybranych przykładach	Student potrafi zidentyfikować rodzaje zagrożeń cyfrowych na wybranych przykładach oraz zaproponować główne działania mitygujące	Student potrafi zidentyfikować rodzaje zagrożeń cyfrowych na wybranych przykładach oraz zaproponować kompleksowe działania mitygujące
PEU_K01	Student aktywnie uczestniczy w pracy zespołu	Student dodatkowo inspirowuje innych	Student dodatkowo potrafi pełnić rolę lidera zespołu

LITERATURA PODSTAWOWA

- 1) Banasiński C. (red), Cyberbezpieczeństwo. Zarys wykładu, Wolters Kluwer, 2023
- 2) Sengal K., Thymianis N., Cyberbezpieczeństwo i strategie blue teamów. Walka z cyberzagrożeniami w Twojej organizacji, Wydawnictwo Helion, 2024

LITERATURA UZUPEŁNIAJĄCA

- 1) Clarkson K., Cyberbezpieczeństwo. Poradnik dla każdego jak chronić się przed zagrożeniem online, Mobilink Konrad Gawroński, 2024
- 2) Zaufanie i cyberbezpieczeństwo w świecie zakupów online, praca zbiorowa, Wydawnictwo SkillsLab, 2024

ŹRÓDŁA INTERNETOWE

Portale branżowe

MACIERZ POWIĄZANIA

EFEKTÓW KSZTAŁCENIA DLA PRZEDMIOTU PODSTAWY CYBERBEZPIECZEŃSTWA

Z EFEKTAMI UCZENIA NA KIERUNKU ZARZĄDZANIE

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	C1	K1-K5	1
PEU_W02	K_W02	C1	K1-K5	1

PEU_U01	K_U01	C1, C2	K1-K5	1
PEU_K01	K_K04	C1, C2	K1-K5	1