

KARTA ZAJĘĆ (SYLABUS)

(forma uproszczona)

Bezpieczny internet**1. Zajęcia i ich usytuowanie w harmonogramie realizacji programu**

1. Jednostka prowadząca kierunek studiów	Zajęcia ogólnouczelniane
2. Nazwa kierunku studiów	
3. Forma prowadzenia studiów	stacjonarne
4. Profil studiów	praktyczny
5. Poziom studiów	I stopnia
6. Nazwa zajęć	<i>Przedmiot wybieralny II: Bezpieczny internet</i>
7. Kod zajęć	
8. Poziom/kategoria zajęć	zajęcia kształcenia ogólnego
9. Status zajęć	fakultatywny
10. Usytuowanie zajęć w harmonogramie realizacji zajęć	Rok I, semestr 2
11. Język wykładowy	polski
12. Liczba punktów ECTS	1

2. Formy zajęć dydaktycznych i ich wymiar w harmonogramie realizacji programu studiów

Wykład W	Ćwiczenia C	Laboratorium L	Projekt P	Konwersatorium K	Praktyka PZ	Inne
-	15	-	-	-	-	-

3. Cele zajęć

	C1	Podniesienie świadomości w zakresie zagrożeń internetowych i cyberbezpieczeństwa.
	C2	Rozwinięcie umiejętności bezpiecznego korzystania z narzędzi i usług online.

4. Wymagania wstępne w zakresie wiedzy, umiejętności i innych kompetencji

Brak

5. Efekty uczenia się dla zajęć, wraz z odniesieniem do efektów uczenia się określonych dla kierunku		
Lp.	Opis efektów uczenia się dla zajęć	Odniesienie do efektów uczenia się określonych dla kierunku - identyfikator efektów uczenia się
W_01	Student zna i rozumie podstawowe zagrożenia związane z korzystaniem z internetu oraz mechanizmy ochrony przed cyberatakami.	K_W03
W_02	Student posiada wiedzę na temat bezpiecznego korzystania z narzędzi i usług online, w tym zarządzania hasłami i rozpoznawania potencjalnie niebezpiecznych stron internetowych.	K_W04
U_01	Student potrafi identyfikować i reagować na zagrożenia internetowe.	K_U05
U_02	Student umie stosować zasady bezpiecznego korzystania z narzędzi i usług online.	K_U02
U_03	Student potrafi oceniać wiarygodność stron internetowych i aplikacji.	K_U09
K_01	Student jest świadomy znaczenia odpowiedzialnego korzystania z technologii i podejmuje działania mające na celu minimalizację potencjalnych zagrożeń.	K_K01

6. Treści kształcenia – oddzielnie dla każdej formy zajęć dydaktycznych							
Ćwiczenia							
Lp.	Tematyka zajęć – szczegółowy opis bloków tematycznych	Liczba godzin					
C01	Wprowadzenie do cyberbezpieczeństwa	2					
C02	Zarządzanie tożsamością i ochroną danych online	3					
C03	Rozpoznawanie zagrożeń internetowych	2					
C04	Praktyki bezpiecznego korzystania z usług online	3					
C05	Reagowanie na incydenty cyberbezpieczeństwa	3					
C06	Etyczne aspekty korzystania z internetu i technologii	2					
Razem		15					
7. Metody weryfikacji efektów uczenia się /w odniesieniu do poszczególnych efektów							
Forma weryfikacji							
Symbol efektu uczenia się	Egzamin ustny	Egzamin pisemny	Kolokwium	Projekt	Sprawdzian wejściowy	Sprawozdanie	Inne:
W_01				X			- Aktywność na zajęciach - Wykonanie zadań praktycznych - Przygotowanie do zajęć - Obserwacja
W_02				X			
U_01				X			
U_02				X			
U_03							
K_01							

8. Obciążenie pracą studenta		
	Forma aktywności	Średnia liczba godzin na zrealizowanie aktywności
	Udział w wykładach	-
	Udział w ćwiczeniach	15
	Udział w konwersatoriach/laboratoriach/projektach	-
	Udział w praktyce zawodowej	-
	Udział nauczyciela akademickiego w egzaminie	-
	Udział w konsultacjach	1
	Suma godzin, w ramach zajęć prowadzonych z bezpośrednim udziałem nauczycieli akademickich lub innych osób prowadzących zajęcia	15
	Samodzielne przygotowanie do zajęć innych niż kształtujące umiejętności praktyczne	-
	Samodzielne przygotowanie do zajęć kształtujących umiejętności praktyczne	10
	Przygotowanie do konsultacji	-
	Przygotowanie do egzaminu i kolokwium	-
	Suma godzin pracy własnej studenta	-
	Sumaryczne obciążenie studenta	10
	Liczba punktów ECTS za zajęcia	1
	Obciążenie studenta zajęciami kształtującymi umiejętności praktyczne	25
	Liczba punktów ECTS za zajęcia kształtujące umiejętności praktyczne	1
	Liczba godzin zajęć prowadzonych z wykorzystaniem metod i technik kształcenia na odległość	8
	Liczba punktów ECTS przypisana do zajęć prowadzonych z wykorzystaniem metod i technik kształcenia na odległość	0,5
(Forma rozszerzona)		
9. Narzędzia dydaktyczne (z uwzględnieniem metod i technik kształcenia na odległość)		
	Symbol	Forma zajęć
	N1	Prezentacja
	N2	Ćwiczenia
	N3	Projekt
10. Ocena osiągniętych efektów uczenia się		
10.1. Sposoby oceny		
	Ocena formująca	
	F1	Obecność na zajęciach.
	F2	Aktywność.
	F3	Terminowe wykonanie zadań praktycznych.
	F4	Przygotowanie do zajęć.
	Ocena podsumowująca	
	P1	Projekt

10.2. Kryteria oceny							
Symbol efektu uczenia	Na ocenę 3	Na ocenę 3,5	Na ocenę 4	Na ocenę 4,5	Na ocenę 5		
W_01 - W_02	Student zna podstawowe zagrożenia i mechanizmy ochrony, ale jego wiedza jest fragmentaryczna.	Student zna zagrożenia i mechanizmy ochrony, ale nie potrafi ich w pełni wyjaśnić.	Student dobrze rozumie zagrożenia i mechanizmy ochrony, potrafi je omówić w sposób przemyślany.	Student zna i rozumie szczegółowe mechanizmy ochrony, potrafi je analizować.	Student wykazuje dogłębną wiedzę na temat zagrożeń i zaawansowanych technik ochrony, zna ich szczegółowe mechanizmy.		
U_01 - U_03	Student stosuje podstawowe techniki ochrony, ale jego działania są niesystematyczne.	Student stosuje techniki ochrony, ale wymaga poprawy w dokładności.	Student efektywnie stosuje techniki ochrony i potrafi reagować na zagrożenia.	Student stosuje techniki ochrony z pewną kreatywnością, jego działania są przemyślane.	Student skutecznie i kreatywnie stosuje zaawansowane techniki ochrony, rozwiązuje problemy cyberbezpieczeństwa.		
K_01	Student zna podstawowe zasady odpowiedzialnego korzystania z technologii, ale jego działania są ograniczone.	Student wykazuje świadomość etycznych aspektów technologii, ale wymaga dalszego rozwinięcia.	Student wykazuje odpowiedzialność i krytyczne myślenie w korzystaniu z technologii.	Student potrafi krytycznie analizować etyczne aspekty technologii i promować odpowiedzialne korzystanie.	Student aktywnie promuje odpowiedzialne korzystanie z technologii, przeprowadza dogłębną analizę etycznych konsekwencji.		

11. Literatura podstawowa i uzupełniająca

Literatura podstawowa:
Banasieński, C. (Red.). (2023). Cyberbezpieczeństwo. Zarys wykładu (2. wyd.). Wolters Kluwer Polska.

Literatura uzupełniająca:
Clarkson, K. (2024). Cyberbezpieczeństwo: Jak chronić się przed phishingiem, cyberstalkingiem, cardingiem, ransomware, hakowaniem, malware, cyberstalkingiem, kradzieżą tożsamości. Helion.

12. Macierz realizacji zajęć

	Symbol efektu uczenia się	Odniesienie efektu do efektów zdefiniowanych dla programu	Cele zajęć	Treści programowe	Narzędzia dydaktyczne	Sposoby oceny	
	W_01	W_03	C1	C01 – C6	N 1 - N 4	F1 - F4	
	W_02	W_04	C1				
	U_01	U_05	C1-C2				
	U_02	U_02	C1-C2				
	U_03	U_09	C1-C2				
	K_01	K_01	C1-C2				

Przemyśl, dnia

Koordynator zajęć	dr Robert Oliwa, prof. PANS	
Odpowiedzialny za realizację zajęć	dr Robert Oliwa, prof. PANS	
Przyjął do realizacji	Podpis osoby odpowiedzialnej za realizację zajęć	
Zatwierdzam	Podpis dyrektora instytutu	