

KARTA PRZEDMIOTU

I. OGÓLNE INFORMACJE O PRZEDMIOCIE						
PAŃSTWOWA WYŻSZA SZKOŁA ZAWODOWA IM. WITELONA W LEGNICY WYDZIAŁ NAUK SPOŁECZNYCH I HUMANISTYCZNYCH						
Kierunek studiów:		Bezpieczeństwo wewnętrzne				
Profil studiów:		Praktyczny				
Forma studiów:		Stacjonarne/niestacjonarne				
Nazwa przedmiotu:		Bezpieczeństwo w cyberprzestrzeni				
Język wykładowy:		Język polski				
Kod przedmiotu kształcenia:		BW1K07				
Poziom studiów:		pierwszy				
Rok studiów:	II	Formy prowadzenia zajęć i liczba godzin w planie studiów:				
Semestr:	III	Wykład	Ćwiczenia	Warsztaty	Seminarium	Praktyka zawodowa
Liczba punktów ECTS:	2	10/8	-	12/10	-	-
Forma zaliczenia:		Zaliczenie na ocenę				
Wymagania wstępne w zakresie wiedzy oraz umiejętności:		Brak wstępnych wymagań				
II. CELE KSZTAŁCENIA						
Cele kształcenia:						
Cel 1: Zapoznanie z istotą, uwarunkowaniami oraz sposobami kształtowania bezpieczeństwa cybernetycznego. Cel 2: Nabycie wiedzydotyczącej polityki cyberbezpieczeństwa państwa oraz instytucji odgrywających kluczową rolę w tych procesach. Cel 3: Pozyskanie niezbędnej wiedzy w zakresie rozpoznawania zagrożeń w obrębie cyberprzestrzeni, które mają bezpośredni wpływ na bezpieczeństwo światowe, państwowe, korporacyjne, ludzkie, itd. Cel 4: Pozyskanie niezbędnej wiedzy dotyczącej rozpoznawania przestępczości zorganizowanej oraz penalizacji cyberprzestępstw. Cel 5: Nabycie podstawowej wiedzy w zakresie funkcjonowania sieci oraz zagrożeń wynikających z funkcjonowaniem stosunków międzyludzkich w zakresie cyberprzestrzeni.						
III. PRZEDMIOTOWE EFEKTY UCZENIA SIĘ WRAZ Z ODNIESIENIEM DO EFEKTÓW KIERUNKOWYCH ORAZ METODY WERYFIKACJI EFEKTÓW						
Efekt	Student, który zaliczył przedmiot w zakresie:			Odniesienie do efektów kierunkowych	Metody weryfikacji	
wiedzy:						
W01	zna i rozumie uwarunkowania (w tym m.in.: społeczne, instytucjonalne, funkcjonalne, prawne, gospodarcze, polityczne i administracyjne) występujące w otoczeniu wewnętrznym i zewnętrznym systemu bezpieczeństwa w skali międzynarodowej, państwowej, regionalnej i lokalnej			K_W04	Test wiedzy, Przygotowanie prezentacji/ projektu, Obserwacja i ocena postaw studenta	
W02	zna i rozumie wybrane zagadnienia szczegółowe z zakresu nauk o bezpieczeństwie			K_W06	Test wiedzy, Przygotowanie prezentacji/ projektu, Obserwacja i ocena postaw studenta	
umiejętności:						
U01	potrafi poprzez praktyczne wykorzystanie posiadanej wiedzy formułować i rozwiązywać złożone i nietypowe problemy związane z bezpieczeństwem, a także wykonywać zadania typowe dla działalności zawodowej związanej z kierunkiem studiów			K_U01	Test wiedzy, Przygotowanie prezentacji/ projektu, Obserwacja i ocena	

			postaw studenta
kompetencji społecznych:			
K01	jest gotów dozasięgnięcia opinii ekspertów w przypadku problemów z samodzielnym rozwiązaniem problemu	K_K02	Przygotowanie prezentacji/ projektu, Obserwacja i ocena postaw studenta
K02	jest gotów dowypełniania zobowiązań społecznych, w tym inicjowania i współorganizowania działalności na rzecz środowiska społecznego i interesu publicznego	K_K03	Obserwacja i ocena postaw studenta
IV. TREŚCI KSZTAŁCENIA			
Treści kształcenia (tematyka zajęć, zaprezentowana z podziałem na poszczególne formy zajęć z określeniem liczby godzin potrzebnych na ich realizację)			
Wykłady:			
Kod	Tematyka zajęć	Liczba godzin	
W1	Zajęcia wprowadzające do problematyki przedmiotu. Omówienie karty przedmiotu, oczekiwań w stosunku do rygoru dydaktycznego oraz poziomu wiedzy.Podstawowe pojęcia związane z bezpieczeństwem w cyberprzestrzeni.	2/1	
W2	Geneza działań w cyberprzestrzeni. Geneza zjawiskaw ujęciu historycznym. Rozwój społeczeństwa informacyjnego oraz technologii teleinformatycznych. Transgraniczność jako zjawisko powiązane z cyberprzestrzenią. Efekty oddziaływania cyberprzestrzeni na systemy gospodarcze.	2/2	
W3	Cyberprzestrzeń – piątywymiar prowadzenia wojny. Ustalenia szczytu NATO w Warszawie w 2016 r. Cechy cyberwojny. Cyberwojna – ujęcie militarne. Cyberwojna a wojna klasyczna. Cyberkonflikt.	2/2	
W4	Cyberbezpieczeństwo państwa. Krajowy system cyberbezpieczeństwa.	2/2	
W5	Ochrona infrastruktury krytycznej w cyberprzestrzeni. Kolokwium ustne lub test online z wykorzystaniem platformy G Suite.	2/1	
Ćwiczenia:			
Kod	Tematyka zajęć	Liczba godzin	
WT1	Omówienie wojny hybrydowej – praca zespołowa.	2/2	
WT2	Omówienie zagrożeń asymetrycznych – praca zespołowa.	2/2	
WT3	Phishing – zagadnienia praktyczne.Ddos, malware, spam nigeryjski, fałszywa reklama, portale społecznościowe, kradzież tożsamości, botnet.	2/1	
WT4	Płatności internetowe, kryptowaluty. Pranie pieniędzy – studium przypadków.	2/1	
WT5	Pornografia dziecięca i pedofilia – geneza zagrożeń, postępowanie sprawców.	2/2	
WT6	Darknet: TOR, I2P, Freenet.	2/2	
V. METODY KSZTAŁCENIA, NARZĘDZIA DYDAKTYCZNE			
1. Metody kształcenia:np. wykład informacyjny (konwencjonalny), wykład problemowy, wykład konwersatoryjny, opowiadanie, opis, metoda problemowa, sytuacyjna, burza mózgów, metoda projektu, studium przypadku, dyskusja, drama, gry symulacyjne. 2. Narzędzia (środki) dydaktyczne: np.prezentacje multimedialne, film, fotografie, materiały archiwalne, teksty źródłowe, dokumenty, mapy, Internet, rzutniki multimedialne.			
VI. FORMA I KRYTERIA ZALICZENIA PRZEDMIOTU			

Forma zaliczenia przedmiotu. Kryteria ocenyformującej:**1. Pisemny test wiedzy (w tym kolokwium zaliczeniowe z wykorzystaniem platformy G Suite) – kryteria oceny:**

- 91% - 100% - bardzo dobry
- 81% - 90% - dobry plus
- 71% - 80% - dobry
- 61% - 70% - dostateczny plus
- 51% - 60% - dostateczny
- 50% i mniej – niedostateczny

2. Kolokwium ustne – kryteria oceny:

- **5,0 (bardzo dobry)** – skomponowanie i artykulacja samodzielnej wypowiedzi na zadany temat w sposób świadczący o pełnym zrozumieniu pytania i znajomości tematu;wnikliwe omówienie zagadnienia;brak błędów językowych;brak błędów w kompozycji;
- **4,5 (dobry plus)** – skomponowanie i artykulacja samodzielnej wypowiedzi na zadany temat w sposób świadczący o pełnym zrozumieniu pytania i znajomości tematu; pełne omówienie zagadnienia; brak błędów językowych; brak błędów w kompozycji;
- **4,0 (dobry)** – skomponowanie i artykulacja samodzielnej wypowiedzi na zadany temat w sposób świadczący o pełnym zrozumieniu pytania i znajomości tematu; pełne omówienie zagadnienia; drobne błędy językowe; drobne błędy w kompozycji;
- **3,5 (dostateczny plus)** – podjęcie próby skomponowania i artykulacji samodzielnej wypowiedzi na zadany temat w sposób świadczący o co najmniej częściowym zrozumieniu pytania i znajomości tematu; całościowe, choć powierzchowne omówienie zagadnienia; drobne błędy językowe; drobne błędy w kompozycji;
- **3,0 (dostateczny)** – podjęcie próby skomponowania i artykulacji samodzielnej wypowiedzi na zadany temat w sposób świadczący o co najmniej częściowym zrozumieniu pytania i znajomości tematu; częściowe omówienie zagadnienia; drobne błędy językowe; drobne błędy w kompozycji;
- **2,0 (niedostateczny)** – niespełnienie kryteriów właściwych dla oceny: dostateczny (3,0).

3. Obserwacja i ocena postaw studenta wynikających z:

- realizacji zadań przygotowanych w ramach ćwiczeń,
- zaangażowania w pracę grupy,
- zachowań i aktywności w trakcie wykładów i ćwiczeń,
- prowadzenia merytorycznej dyskusji,
- potrzeby ciągłego rozwoju osobistego i zawodowego.

Kryteria oceny podsumowującej:

- średnia ocen formujących

VII. BILANS PUNKTÓW ECTS –NAKŁAD PRACY STUDENTA

Kategoria	Obciążenie studenta
Liczba godzin realizowanych przy bezpośrednim udziale nauczyciela (godziny kontaktowe)	22/18
Udział w wykładach	9/7
Udział w ćwiczeniach, warsztatach	12/10
Udział w seminarium	-
Udział w egzaminie	-
Udział w kolokwium zaliczeniowym	1/1
Samodzielna praca studenta (godziny niekontaktowe)	28/32
Przygotowanie do wykładu	4/4
Przygotowanie do ćwiczeń, warsztatów,	10/8
Przygotowanie do kolokwium zaliczeniowego	4/6
Przygotowanie do egzaminu	-
Przygotowanie do seminarium	-
Gromadzenie materiałów do projektu	4/4
Kwerenda internetowa	3/5
Opracowanie prezentacji multimedialnej	3/5
Przygotowanie do praktyki zawodowej	-
Inne (jakie?)	-

Łączna liczba godzin	50/50
Punkty ECTS za przedmiot	2
VIII. LITERATURA PRZEDMIOTU	
Literatura podstawowa: 1.C. Banasiński, Cyberbezpieczeństwo – zarys wykładu, Wolters Kluwer, Warszawa 2018. 2.Ustawaz dnia 5 lipca 2018 r.o krajowym systemie cyberbezpieczeństwa, DzU z 2018, poz. 1369.	
Literatura uzupełniająca: 1.J. Kosiński – Paradygmaty cyberprzestępczości; wyd. I, wyd. Difin SA, Warszawa 2015. 2. K. Linderman – Bezpieczeństwo informacyjne. Nowe wyzwania; wyd. II, wyd. PWN SA, Warszawa 2017. 3.Doktryna cyberbezpieczeństwa RP, Warszawa 2015. 4. https://rcb.gov.pl/	