Załącznik nr 5

KARTA PRZEDMIOTU

I. Dane podstawowe

Nazwa przedmiotu	Analiza konfliktów z cyberbezpieczeństwa
Nazwa przedmiotu w języku angielskim	Cybersecurity related analysis of conflicts
Kierunek studiów	Bezpieczeństwo narodowe
Poziom studiów (I, II, jednolite magisterskie)	II stopień
Forma studiów (stacjonarne, niestacjonarne)	Stacjonarne
Dyscyplina	Nauki o polityce i administracji, Nauki o Bezpieczeństwie
Język wykładowy	Polski

Koordynator przedmiotu/osoba odpowiedzialna	Urszula Soler

Forma zajęć *(katalog zamknięty ze słownika)*	Liczba godzin	semestr	Punkty ECTS
wykład			4
konwersatorium			
ćwiczenia	30	I	
laboratorium			
warsztaty			
seminarium			
proseminarium			
lektorat			
praktyki			
zajęcia terenowe			
pracownia dyplomowa			
translatorium			
wizyta studyjna			

Wymagania wstępne	Znajomość podstawowych podstawowych pojęć z zakresu cyberbezpieczeństwa

II. Cele kształcenia dla przedmiotu

C1 - Zapoznanie z głównymi zagadnieniami dotyczącymi cyberbezpieczeństwa
C2 - Przekazanie wiedzy nt. sposobów przebiegów konfliktów z cyberprzestrzeni i analizy ich rozwoju
C3 - Ukierunkowanie na potrzebę samodzielnego, krytycznego analizowania zjawisk w obszarze

III. Efekty uczenia się dla przedmiotu wraz z odniesieniem do efektów kierunkowych

Symbol	Opis efektu przedmiotowego	Odniesienie do efektu kierunkowego
WIEDZA		
W_01	Zna złożony charakter uwarunkowań bezpieczeństwa globalnego, systemów bezpieczeństwa państwa, a także bezpieczeństwa międzynarodowego, w tym instytucji międzynarodowych	K_W05
W_02	Zna i definiuje zjawiska w obszarze cyberbezpieczeństwa	K_W03
UMIEJĘTNOŚCI		
U_01	Potrafi wykorzystywać pogłębioną wiedzę teoretyczną w rozwiązywaniu problemów związanych z cyberbezpieczeństwem państwa i w wymiarze międzynarodowym	K_U03
U_02	Potrafi prawidłowo oceniać zagrożenia w cyberprzestrzeni, a także identyfikować ich przyczyny	K_U05
KOMPETENCJE SPOŁECZNE		
K_01	Jest gotów do angażowania się w działania wspierające procesy bezpieczeństwa międzynarodowego w cyberprzestrzeni	K_K01, K_K02

IV. Opis przedmiotu/ treści programowe

1. Bezpieczeństwo w cyberprzestrzeni – historia cyberprzestrzeni i prognozy przyszłości cyberprzestrzeni, definicja zagrożeń cybernetycznych, problem rozróżnienia ataków cybernetycznych 2. Bezpieczeństwo w erze Big Data – konsekwencje analizy wielkich zbiorów danych, możliwe naruszenia prawa do prywatności, prawo do bycia zapomnianym, bezpieczeństwo danych osobowych, RODO/GDPR w praktyce 3. Wojna w cyberprzestrzeni – problem atrybucji ataku cybernetycznego, prawne aspekty wojny w cyberprzestrzeni, kontrowersje na temat możliwości prowadzenia wojny w cyberprzestrzeni 4. Rewolucja IT w kontekście militarnym - przyszłość Internetu, nowy „cybernetyczny" żołnierz, IoT, sztuczna inteligencja, Big Data, AR na użytek wojska 5. Cyberprzestrzeń jako wymiar rywalizacji państw (Chiny, USA, UE, NATO…) wywiad cybernetyczny, rywalizacja gospodarcza/wywiad gospodarczy, Internet jako narzędzie propagandy

V. Metody realizacji i weryfikacji efektów uczenia się

Symbol efektu	Metody dydaktyczne *(lista wyboru)*	Metody weryfikacji *(lista wyboru)*	Sposoby dokumentacji *(lista wyboru)*
WIEDZA			
W_01	Ćwiczenia	Zaliczenie	protokół
UMIEJĘTNOŚCI			
U_01	Ćwiczenia Analiza aktualnych konfliktów w cyberprzestrzeni i tekstów źródłowych w Internecie	Zaliczenie	protokół

U_02	Ćwiczenia Studium przypadku	Zaliczenie	protokół
KOMPETENCJE SPOŁECZNE			
K_01	Dyskusja stacjonarna	Zaliczenie	protokół

VI. Kryteria oceny, wagi…

Systematyczna obecność na zajęciach i aktywność na nich. Udział w wydarzeniach (konferencje, seminaria) związanych z tematyką zajęć. Zaliczenie ćwiczeń.

VII. Obciążenie pracą studenta

Forma aktywności studenta	Liczba godzin
Liczba godzin kontaktowych z nauczycielem	**30**
Liczba godzin indywidualnej pracy studenta	**15**

VIII. Literatura

Literatura podstawowa
M. Wrzosek, Operacje w cyberprzestrzeni. Założenia teoretyczne i praktyka, Kwartalnik Bellona 2016; 687 (4): 42-59. D. Van Puyvelde , A. F. Brantly, Cybersecurity: Politics, Governance and Conflict in Cyberspace 1st Edition, Polity; 1st edition (September 3, 2019).
Literatura uzupełniająca
K. Chałubińska-Jentkiewicz, The Role of Cybersecurity in the Public Sphere - The European Dimension, Lex Localis, Maribor, 2022. M. B. Gazula, Cyber Warfare Conflict Analysis and Case Studies, Massachusetts Institute of Technology June 2017. M. Karpiuk, U. Soler, A. Makuch, Rola Strategii Cyberbezpieczeństwa RP w zakresie zapewnienia bezpieczeństwa w cyberprzestrzeni, “Polish Political Science Yearbook”.