KARTA KURSU

Nazwa	Międzynarodowe bezpieczeństwo informacyjne

Kod		Punktacja ECTS*	3

Koordynator	Dr Agnieszka Warchoł	Zespół dydaktyczny

Opis kursu (cele kształcenia)

Celem kursu jest zapoznanie studentów z koncepcją międzynarodowego bezpieczeństwa informacyjnego oraz wskazanie podstawowych międzynarodowych regulacji prawnych w zakresie bezpieczeństwa informacyjnego, w tym cyberbezpieczeństwa. Na kursie omówiona zostanie współpraca międzynarodowa, ale także problem atrybucji ataku cybernetycznego oraz prawne aspekty wojny w cyberprzestrzeni, co wiąże się z ofensywnym wykorzystaniem cyberprzestrzeni na arenie stosunków międzynarodowych. Dodatkowo, w perspektywie porównawczej zostaną przedstawione polityki cyberbezpieczeństwa wybranych państw.

Warunki wstępne

Wiedza	-
Umiejętności	-
Kursy	-

Efekty kształcenia

	Efekt kształcenia dla kursu	Odniesienie do efektów kierunkowych
Wiedza	W 01 Ma wiedzę o istocie międzynarodowej współpracy w zakresie bezpieczeństwa informacyjnego, jej znaczeniu dla bezpieczeństwa w wymiarze międzynarodowym. W 02 Wskazuje główne międzynarodowe regulacje prawne w zakresie bezpieczeństwa informacyjnego. W 03 Potrafi scharakteryzować i porównać polityki cyberbezpieczeństwa wybranych państw.	BI_W01, BI_W02, - BI_W03, BI_W04

Umiejętności	Efekt kształcenia dla kursu	Odniesienie do efektów kierunkowych

	U 01 Potrafi wykorzystać wiedzę teoretyczną do opisu i analizy zjawisk z zakresu międzynarodowego bezpieczeństwa informacyjnego. U 02 Potrafi pozyskiwać informacje, wykorzystywać nowoczesne technologie oraz media dla zapewnienia bezpieczeństwa informacyjnego. U 03 Potrafi zarządzać informacją i przedstawić efekty swojej pracy w sposób zrozumiały i logiczny.	BI_U01, BI_U02, BI_U03

	Efekt kształcenia dla kursu	Odniesienie do efektów kierunkowych
Kompetencje społeczne	K 01 Rozumie potrzebę zdobywania wiedzy i doskonalenia kompetencji w zakresie międzynarodowego bezpieczeństwa informacyjnego. K 02 Umie pracować w grupie. K 03 Potrafi samodzielnie i krytycznie oceniać własne kompetencje oraz działać racjonalnie i etycznie.	BI_K01, BI_K02, BI_K03

Forma zajęć	Organizacja						
	Wykład (W)	Ćwiczenia w grupach					
		A	K	L	S	P	E
Liczba godzin	10	10					

Opis metod prowadzenia zajęć

Ćwiczenia:
- analiza źródeł, analiza literatury przedmiotu,
- *case study*,
- dyskusja,
- referaty w grupach.

Wykład monograficzny z wykorzystaniem prezentacji multimedialnej.

Formy sprawdzania efektów kształcenia

	E – learning	Gry dydaktyczne	Ćwiczenia w szkole	Zajęcia terenowe	Praca laboratoryjna	Projekt indywidualny	Projekt grupowy	Udział w dyskusji	Referat	Praca pisemna (esej)	Egzamin ustny	Egzamin pisemny	Inne
W01	X						X	X	X			X	
W02	X						X	X	X			X	

W03	X						X	X	X			X	
U01	X						X	X	X			X	
U02	X						X	X	X			X	
U03	X						X	X	X			X	
K01	X						X	X	X				
K02	X						X	X	X				
K03	X						X	X	X				

Kryteria oceny	Ćwiczenia - obecność (dopuszczalna jedna nieobecność nieusprawiedliwiona), - aktywność przejawiająca się w znajomości tekstów rekomendowanych przez prowadzącą, - referat na wybrany temat. Wykład Egzamin pisemny. Warunkiem dopuszczenia do egzaminu jest zaliczenie ćwiczeń.

Uwagi	Indywidualny program studiów – warunki zaliczenia ustalane indywidualnie z prowadzącą zajęcia po przedstawieniu zgody na indywidualny tok studiów.

Treści merytoryczne (wykaz tematów)

Wykłady

1. Zajęcia organizacyjne. Przedstawienie warunków zaliczenia przedmiotu.
2. Koncepcja międzynarodowego bezpieczeństwa informacyjnego. Współpraca międzynarodowa w zakresie cyberbezpieczeństwa.
3. Międzynarodowe regulacje prawne w zakresie bezpieczeństwa informacyjnego, w tym cyberbezpieczeństwa.
4. Cyberprzestrzeń jako wymiar rywalizacji państw. Wybrane aspekty.
5. Ofensywne wykorzystanie cyberprzestrzeni na arenie stosunków międzynarodowych. Problem atrybucji ataku cybernetycznego, prawne aspekty wojny w cyberprzestrzeni. Tallin Manual.
6. Polityki cyberbezpieczeństwa wybranych państw.

Ćwiczenia:

1. Wpływ podmiotów zewnętrznych na bezpieczeństwo procesów wyborczych. Wnioski po wyborach parlamentarnych 2023 r. w Polsce.
2. Rola mediów społecznościowych w kreowaniu środowiska bezpieczeństwa międzynarodowego.
3. Cyberarmie we współczesnym świecie. Perspektywa porównawcza – wybrane przykłady.
4. Wojna Rosji z Ukrainą – działania w cyberprzestrzeni.
5. Nowe trendy w cyberbezpieczeństwie.
6. Prognozowanie przyszłości cyberprzestrzeni i jej roli w przyszłych konfliktach zbrojnych.

Wykaz literatury podstawowej

Obowiązkujące akty prawne i strategie.
Dela P.T., *Założenia działań w cyberprzestrzeni,* PWN, Warszawa 2022.
Rydlewski G., *Rządzenie w epoce informacji, cyfryzacji i sztucznej inteligencji*, Elipsa, Warszawa 2021.
Banasiński C. (red.), *Cyberbezpieczeństwo. Zarys wykładu*, Wolters Kluwers, Warszawa 2018.
Routledge Companion to Global Cyber-Security Strategy, Scott N. Romaniuk, Mary Manijikian (ed.), Routledge NY, 2020

Wykaz literatury uzupełniającej

Siudak R., *Cyberbezpieczeństwo w Polsce. Od dyskursów do polityk publicznych*, Wydawnictwo Księgarnia Akademicka, Kraków 2022.
Choucri N., Clark David D., *International Relations in the Cyber Age. The Co-Evolution Dilemma*, MIT 2018.
Hoffmann T., *Wybrane aspekty cyberbezpieczeństwa w Polsce,* Poznań 2018.
Klimburg A., *The Darkening Web. The War for Cyberspace*, NY 2017.
Lakomy, M., *Cyberprzestrzeń jako nowy wymiar rywalizacji i współpracy państw*, Wydawnictwo Uniwersytetu Śląskiego, Katowice 2015.
Liderman K., *Bezpieczeństwo informacyjne. Nowe wyzwania*, PWN, Warszawa 2017.
Warchoł A., Wpływ cyberprzestrzeni na bezpieczeństwo państwa na początku XXI wieku (praca doktorska), Kraków 2017(wybrane fragmenty).
Ball M., *Metawersum. Jak internet przyszłości zrewolucjonizuje świat i biznes*, Warszawa 2022.
Kitler W., Taczkowska-Olszewska J., Radoniewicz F. (red.), *Ustawa o krajowym systemie cyberbezpieczeństwa. Komentarz*, C.H.Beck, Warszawa 2019.
Kreft J., *Władza platform. Za fasadą Google, Facebooka i Spotify*, Kraków 2021.
Libicki M.C., *Cyberdeterrence and Cyberwar, RAND Corporation*, Santa Monica, CA 2009.
Marczewska-Rytko M. (red.), *Haktywizm (cyberterroryzm, haking, protest obywatelski, cyberaktywizm, e-mobilizacja*, Lublin 2014.
Olejnik Ł, Kurasiński A., *Filozofia cyberbezpieczeństwa. Jak zmienia się świat? Od złośliwego oprogramowania do cyberwojny*, PWN, Warszawa 2022.
Rid T., *Wojna informacyjna*, Warszawa 2020.
The Tallinn Manual 2.0
Vademecum bezpieczeństwa informacyjnego (wybór haseł).
Zuboff S., *Wiek kapitalizmu inwigilacji. Walka o przyszłość ludzkości na nowej granicy władzy,* Wydawnictwo Zysk i S-ka, Poznań 2020.
Warchoł A., *Ochrona praw i wolności w dobie Internetu*, [w:] *Cyberprzestrzeń jako pole zmagań o bezpieczeństwo informacyjne*, (red.) W. Fehler, Siedlce 2022.

Bilans godzinowy zgodny z CNPS (Całkowity Nakład Pracy Studenta)

liczba godzin w kontakcie z prowadzącymi	Wykład	10
	Konwersatorium (ćwiczenia, laboratorium itd.)	10

	Pozostałe godziny kontaktu studenta z prowadzącym	
liczba godzin pracy studenta bez kontaktu z prowadzącymi	Lektura w ramach przygotowania do zajęć	20
	Przygotowanie krótkiej pracy pisemnej lub referatu po zapoznaniu się z niezbędną literaturą przedmiotu	
	Przygotowanie projektu lub prezentacji na podany temat (praca w grupie)	15
	Przygotowanie do egzaminu/zaliczenia	20
Ogółem bilans czasu pracy		75
Liczba punktów ECTS w zależności od przyjętego przelicznika		3