

KARTA KURSU
(realizowanego w specjalności)
CYBERBEZPIECZEŃSTWO
(nazwa specjalności)

Nazwa	Stosunki międzynarodowe w cyberprzestrzeni
-------	--

Kod		Punktacja ECTS*	3
-----	--	-----------------	---

Koordynator	Dr Agnieszka Warchoł	Zespół dydaktyczny
-------------	----------------------	--------------------

Opis kursu (cele kształcenia)

Celem kursu jest zapoznanie studentów z rolą cyberprzestrzeni w stosunkach międzynarodowych oraz wskazanie podstawowych międzynarodowych regulacji prawnych w zakresie bezpieczeństwa informacyjnego, w tym cyberbezpieczeństwa. Na kursie omówiona zostanie współpraca międzynarodowa, ale także problem atrybucji cyberataku 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 uczenia się

	Efekt uczenia się dla kursu	Odniesienie do efektów kierunkowych
Wiedza	<p>W01: ma wiedzę o istocie międzynarodowej współpracy w zakresie bezpieczeństwa informacyjnego, jej znaczenia dla bezpieczeństwa w wymiarze międzynarodowym.</p> <p>W02: Wskazuje główne międzynarodowe regulacje prawne w zakresie bezpieczeństwa informacyjnego.</p> <p>W03: Ma wiedzę o roli cyberprzestrzeni w stosunkach międzynarodowych</p>	SC_W06, SC_W07

	Efekt uczenia się dla kursu	Odniesienie do efektów kierunkowych
Umiejętności	U01: Potrafi wykorzystać wiedzę teoretyczną do opisu i analizy zjawisk z zakresu stosunków międzynarodowych w cyberprzestrzeni.	SC_U09, SC_U10
	U02: Potrafi pozyskiwać informacje, wykorzystywać nowoczesne technologie oraz media dla zapewnienia bezpieczeństwa informacyjnego.	
	U03: Potrafi zarządzać informacją i przedstawić efekty swojej pracy w sposób zrozumiały o logiczny.	

	Efekt kształcenia dla kursu	Odniesienie do efektów kierunkowych
Kompetencje społeczne	K 01 Rozumie potrzebę zdobywania wiedzy i doskonalenia kompetencji w zakresie cyberbezpieczeństwa z uwzględnieniem aspektów dotyczących stosunków międzynarodowych.	SC_K02, SC_K03
	K 02 Umie pracować w grupie.	
	K 03 Potrafi samodzielnie i krytycznie oceniać własne kompetencje oraz działać racjonalnie i etycznie.	

Studia stacjonarne

Organizacja											
Forma zajęć	Wykład (W)	Ćwiczenia w grupach									
		A		K		L		S		P	E
Liczba godzin	15	15									

Studia niestacjonarne

Organizacja											
Forma zajęć	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				
W02	X						X	X	X				
W03	X						X	X	X				
U01	X						X	X	X				
U02	X						X	X	X				
U03	X						X	X	X				
K01	X						X	X	X				
K02	X						X	X	X				
K03	X						X	X	X				

Kryteria oceny	<p>Ćwiczenia</p> <ul style="list-style-type: none"> - obecność (dopuszczalna jedna nieobecność nieusprawiedliwiona), - aktywność przejawiająca się w znajomości tekstów rekomendowanych przez prowadzącą, - referat na wybrany temat. <p>Wykład (Zaliczenie bez oceny)</p>
----------------	---

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 i omówienie literatury przedmiotu.
2. Stosunki międzynarodowe w cyberprzestrzeni.
3. Współpraca międzynarodowa w zakresie cyberbezpieczeństwa.
4. Międzynarodowe regulacje prawne w zakresie bezpieczeństwa informacyjnego, w tym cyberbezpieczeństwa.
5. Cyberprzestrzeń jako wymiar rywalizacji państw. Wybrane aspekty.
6. Ofensywne wykorzystanie cyberprzestrzeni na arenie stosunków międzynarodowych. Problem atrybucji ataku cybernetycznego, prawne aspekty wojny w cyberprzestrzeni. Tallin Manual.
7. Polityki cyberbezpieczeństwa wybranych państw.

Ćwiczenia:

1. Zajęcia organizacyjne. Przedstawienie warunków zaliczenia i omówienie literatury przedmiotu.
2. 2024 rok jako rok wyborczy. Wpływ podmiotów zewnętrznych na bezpieczeństwo procesów wyborczych w państwach.
3. Rola mediów społecznościowych w kreowaniu środowiska bezpieczeństwa międzynarodowego.
4. Cyberarmie we współczesnym świecie. Perspektywa porównawcza – wybrane przykłady.
5. Wojna Rosji z Ukrainą – działania w cyberprzestrzeni.
6. Prawa i wolności człowieka w dobie Internetu.
7. Prognozowanie przyszłości cyberprzestrzeni i jej roli w przyszłych konfliktach zbrojnych.

Wykaz literatury podstawowej

Obowiązujące akty prawne i strategie.

Banasiński C. (red.), *Cyberbezpieczeństwo. Zarys wykładu*, Wolters Kluwers, Warszawa 2023

Dela P.T., *Założenia działań w cyberprzestrzeni*, PWN, Warszawa 2022.

Rydlewski G., *Rządzenie w epoce informacji, cyfryzacji i sztucznej inteligencji*, Elipsa, Warszawa 2021.

Routledge Companion to Global Cyber-Security Strategy, Scott N. Romaniuk, Mary Manijkian (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.

Warchoń 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., Taczowska-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-Rytka M. (red.), *Haktywizm (cyberterrorizm, haking, protest obywatelski, cyberaktywizm, emobilizacja)*, Lublin 2014.

Olejniak 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 Zys i S-ka, Poznań 2020.

Warchoń A., *Ochrona praw i wolności w dobie Internetu*, [w:] *Cyberprzestrzeń jako pole zmagania o bezpieczeństwo informacyjne*, (red.) W. Fehler, Siedlce 2022.

Bilans godzinowy zgodny z CNPS (Całkowity Nakład Pracy Studenta) - **studia stacjonarne**

liczba godzin w kontakcie z prowadzącymi	Wykład	15
	Konwersatorium (ćwiczenia, laboratorium itd.)	15
	Pozostałe godziny kontaktu studenta z prowadzącym	
liczba godzin pracy studenta bez kontaktu z prowadzącymi	Lektura w ramach przygotowania do zajęć	15
	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	15
Ogółem bilans czasu pracy		75
Liczba punktów ECTS w zależności od przyjętego przelicznika		3

Bilans godzinowy zgodny z CNPS (Całkowity Nakład Pracy Studenta) - **studia niestacjonarne**

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	15
	Przygotowanie krótkiej pracy pisemnej lub referatu po zapoznaniu się z niezbędną literaturą przedmiotu	
	Przygotowanie projektu lub prezentacji na podany temat (praca w grupie)	20
	Przygotowanie do egzaminu/zaliczenia	20
Ogółem bilans czasu pracy		75
Liczba punktów ECTS w zależności od przyjętego przelicznika		3