KARTA KURSU

Nazwa	Społeczne aspekty cyberbezpieczeństwa
Nazwa w j. ang.	The social aspects of cyber security

Kod		Punktacja ECTS*	2

Koordynator	dr Agnieszka Warchoł	Zespół dydaktyczny

Opis kursu (cele kształcenia)

Celem kursu jest zapoznanie studentów z podejściem do cyberbezpieczeństwa osadzonym w naukach społecznych. Poznanie istoty cyberprzestrzeni, zagrożeń, szans i wyzwań w zakresie cyberbezpieczeństwa państwa. Spojrzenie na cyberprzestrzeń przez pryzmat praw i wolności człowieka i obywatela.

Efekty kształcenia

	Efekt kształcenia dla kursu	Odniesienie do efektów kierunkowych
Wiedza	Student posiada zaawansowaną wiedzę w zakresie bezpieczeństwa państwa, w tym cyberbezpieczeństwa, jako nauki oraz wiedzę o jej miejscu i roli w obszarze nauk społecznych. Zna podstawowe pojęcia w zakresie cyberbezpieczeństwa.	K1_W01
	Dysponuje zasadniczą wiedzą o człowieku jako podmiocie uczestniczącym w procesie kształtowania środowiska cyberbezpieczeństwa państwa	K1_W03
	Posiada podstawową wiedzę i rozumie konieczność stałego poznawania ewolucji procesów, struktur i instytucji właściwych w sferze cyberbezpieczeństwa państwa.	K1_W06

Umiejętności	Efekt kształcenia dla kursu	Odniesienie do efektów kierunkowych

	Student potrafi dostrzec, prawidłowo ocenić, a następnie dokonać interpretacji zjawisk w zakresie cyberbezpieczeństwa, patrząc na nie poprzez pryzmat procesów: historycznych, politycznych, społecznych, gospodarczych, militarnych, działalności zorganizowanych grup przestępczych, cyberterroryzmu, a także rozumiejąc konieczność stałego zgłębiania wiedzy w tym zakresie.	K1_U01
	W sposób prawidłowy potrafi zastosować pojęcia z zakresu nauk społecznych, w szczególności dotyczące nomenklatury pojęciowej związanej z cyberbezpieczeństwem.	K2_U02
	Potrafi połączyć w spoistą całość zjawiska kulturowe, społeczne, polityczne, prawne, ekonomiczne, wojskowe i towarzyszące im cyberzagrożenia, które zachodzą w rozumianym otoczeniu wewnętrznym państwa, mające wpływ na bezpieczeństwo państwa.	K2_U02

	Efekt kształcenia dla kursu	Odniesienie do efektów kierunkowych
Kompetencje społeczne	Potrafi myśleć i podejmować działania na podstawie analiz i ocen występujących zjawisk i zdarzeń, które mają wpływ na cyberbezpieczeństwo.	K2_K01
	Potrafi efektywnie analizować i trafnie interpretować przyczyny i przebieg konkretnych procesów i zjawisk społecznych w zakresie cyberbezpieczeństwa.	K2_K02

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

Opis metod prowadzenia zajęć

Dyskusja problemowa w oparciu o teksty wskazane przez prowadzącą. Studenci wygłaszają referaty.

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				
W03							X	X	X				
W06							X	X	X				
U01							X	X	X				
U02							X	X	X				
U02							X	X	X				
K01							X	X	X				
K02							X	X	X				

Kryteria oceny	Na zaliczenie przedmiotu składają się: - obecność na zajęciach (dopuszczalna jedna nieobecność nieusprawiedliwiona), - znajomość tekstów wskazanych przez prowadzącą, - referat na wybrany temat.

Uwagi	Nieobecności odrabiamy podczas dyżuru stacjonarnego lub online.

Treści merytoryczne (wykaz tematów)

1. Zajęcia organizacyjne. Omówienie zasad zaliczenia przedmiotu. Terminologia i zarys problemu. Wybór referatów.
2. Wyzwania dla bezpieczeństwa państwa w cyberprzestrzeni.
3. Zagrożenia dla bezpieczeństwa państwa w cyberprzestrzeni.
4. Cyberwojna – element futurologii czy rzeczywistości?
5. Wpływ cyberprzestrzeni na dyplomację.
6. Ochrona praw i wolności człowieka w dobie Internetu.
7. Podsumowanie.

Wykaz literatury podstawowej

Lakomy M., *Cyberprzestrzeń jako nowy wymiar rywalizacji i współpracy państw*, Katowice 2015.
Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz.U. 2018 poz. 1560).
Sartori G., *Homo videns. Telewizja i postmyślenie*, Warszawa 2007.
Hagen M., *A typology of Electronic Democracy*, http://martin-hagen.net/publikationen/elektronische-demokratie/typology-of-electronic-democracy/.
Kowalewski M., Jakubiak M. (red.), *Współczesne trendy cyberzagrożeń społeczeństwa informacyjnego*, Warszawa 2022.
Broś N., *Znaczenie nowych technologii dla współczesnej dyplomacji.* „Dialogi Polityczne" 2018 [online], nr 22.
Warchoł A., *Ochrona praw i wolności w dobie Internetu*, [w:] *Cyberprzestrzeń jako pole zmagań o bezpieczeństwo informacyjne*, (red.) W. Fehler, Siedlce 2022.

Wykaz literatury uzupełniającej

Angwin J., *Społeczeństwo nadzorowane. W poszukiwaniu prywatności, bezpieczeństwa i wolności w świetle permanentnej inwigilacji*, Warszawa 2017.
Bartlett J., *Ludzie przeciw technologii. Jak Internet zabija demokrację (i jak możemy ją ocalić),* Katowice 2019.
Binicewicz A., *O prywatności w świecie nowych technologii. Asymetria przejrzystości*, Kraków 2021.
DEZINFORMACJA – INSPIRACJA – SPOŁECZEŃSTWO SOCIAL CYBERSECURITY, red. D. Boćkowski, E. Dąbrowska-Prokopowska, P. Goryń, K. Goryń, Białystok 2022. Dostępna tutaj: https://repozytorium.uwb.edu.pl/jspui/bitstream/11320/13835/1/Dezinformacja_Inspiracja_Spoleczenstwo.pdf.
Galloway S., *Wielka czwórka. Ukryte DNA: Amazon, Apple, Facebook i Google*, Poznań 2018.
Kura A., *Zagrożenia dla bezpieczeństwa informacyjnego państwa u progu XXI wieku*, Stalowa Wola 2016.
Libicki M.C., *Cyberdeterrence and Cyberwar, RAND Corporation*, Santa Monica, CA 2009.
Manor I., *The Digitalization of Public Diplomacy, (On Selfie Diplomacy),* s. 257-285.
Olejnik Ł., Kurasiński A., *Filozofia cyberbezpieczeństwa. Jak zmienia się świat? Od złośliwego oprogramowania do cyberwojny*, Warszawa 2022.
Pomarański M., *Haktywizm jako ruch protestu XXI wieku*, [w:] M. Marczewska-Rytko (red.), *Haktywizm (cyberterroryzm, haking, protest obywatelski, cyberaktywizm, e-mobilizacja*, Lublin 2014.
Surmacz B., *Wpływ nowych technologii na funkcje współczesnej demokracji*, [w:] M. Kosienkowski, B. Piskorska (red.) *Dyplomacja cyfrowa jako instrument polityki zagranicznej XXI wieku*, Lublin 2014, s.27-41.
Szpyra R., *Militarne operacje informacyjne*, Warszawa 2003.
Tallinn Manual 2.0. on the International Law Applicable to Cyber Operations.
Twiplomacy 2020, https://twiplomacy.com/blog/twiplomacy-study-2020/
Walsh T., *To żyje! Sztuczna inteligencja. Od ideologicznego fortepianu po zabójcze roboty*, Warszawa 2018.
Warchoł A., *Cybercenzura [w:] Encyklopedia bezpieczeństwa*, t. 1, (red.) O. Wasiuta, S. Wasiuta, Kraków 2021 ,s. 764-767.
Warchoł A., *Cyberwojna – element futurologii czy rzeczywistości?* [w:] E. Fogelzang-Adler, E. Sadowska (red.),Wybrane problemy bezpieczeństwa t. 2, Kraków 2018.
Wylie C., *Mindf*ck. Cambridge Analytica, czyli jak popsuć demokrację*, Kraków 2020.
Zuboff S., *Wiek kapitalizmu inwigilacji. Walka o przyszłość ludzkości na nowej granicy władzy,* Poznań 2020.

Bilans godzinowy zgodny z CNPS (Całkowity Nakład Pracy Studenta)

Ilość godzin w kontakcie z prowadzącymi	Wykład	
	Konwersatorium (ćwiczenia, laboratorium itd.)	10
	Pozostałe godziny kontaktu studenta z prowadzącym	
Ilość 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	10
	Przygotowanie projektu lub prezentacji na podany temat (praca w grupie)	10
	Przygotowanie do egzaminu	
Ogółem bilans czasu pracy		50
Ilość punktów ECTS w zależności od przyjętego przelicznika		2