KARTA KURSU

Nazwa	Bezpieczeństwo w cyberprzestrzeni
Nazwa w j. ang.	Cybersecurity

Kod		Punktacja ECTS*	3

Koordynator	dr Agnieszka Warchoł	Zespół dydaktyczny

Opis kursu (cele kształcenia)

C.1. Poznanie istoty cyberprzestrzeni, zagrożeń, szans i wyzwań w zakresie cyberbezpieczeństwa państwa. Znajomość struktur organizacyjnych, instytucji i norm w zakresie cyberbezpieczeństwa.

C.2. Nabycie umiejętności identyfikowania, przewidywania i analizy zagrożeń dla cyberbezpieczeństwa. Umiejętność interpretacji aktów prawa międzynarodowego, regionalnego i krajowego, związanych z problematyką cyberbezpieczeństwa.

Warunki wstępne

Wiedza	Student zna podstawowe zagadnienia dotyczące bezpieczeństwa w cyberprzestrzeni: terminologia, katalog zagrożeń, podmioty kreujące zagrożenia, zagadnienia prawne, organy odpowiedzialne za cyberbezpieczeństwo w państwie.
Umiejętności	Student posiada umiejętności rozróżniania, identyfikowania i diagnozowania współczesnych zagrożeń, wyzwań i szans dla bezpieczeństwa państwa w cyberprzestrzeni, określania kompetencji działania organów i instytucji odpowiedzialnych za cyberbezpieczeństwo, interpretacji aktów prawnych w zakresie cyberbezpieczeństwa.
Kursy	Bezpieczeństwo państwa.

Efekty kształcenia

Wiedza	Efekt kształcenia dla kursu	Odniesienie do efektów kierunkowych

	K1_W01. Student ma wiedzę dotyczącą istoty i zakresu cyberbezpieczeństwa, zagrożeń dla bezpieczeństwa państwa w cyberprzestrzeni oraz systemu cyberbezpieczeństwa Rzeczypospolitej Polskiej. K2_W02. Posiada pogłębioną wiedzę dotyczącą relacji zachodzących między instytucjami występującymi w otoczeniu wewnętrznym państwa, które mają wpływ na jego cyberbezpieczeństwo. K2_W04. Posiada poszerzoną wiedzę dotyczącą historycznej ewolucji struktur i instytucji związanych z cyberbezpieczeństwem państwa.	P7S_WG P7S_WG P7S_WG

	Efekt kształcenia dla kursu	Odniesienie do efektów kierunkowych
Umiejętności	K2_U01. 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. K2_U02. W sposób prawidłowy potrafi zastosować pojęcia z zakresu nauk społecznych, w szczególności dotyczące nomenklatury pojęciowej związanej z cyberbezpieczeństwem. K2_U06. 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.	P7S_UU P7S_UW P7S_UO

Kompetencje społeczne	Efekt kształcenia dla kursu	Odniesienie do efektów kierunkowych

	K2_K01. Potrafi myśleć i podejmować działania na podstawie analiz i ocen występujących zjawisk i zdarzeń, które mają wpływ na cyberbezpieczeństwo. K2_K02. Umie sukcesywnie uzupełniać zdobytą wiedzę, rozumiejąc konieczność stałego rozwoju w zakresie cyberbezpieczeństwa, jak i doskonalenia umiejętności związanych zarówno z identyfikacją zagrożeń jak i z szansami i wyzwaniami w zakresie bezpieczeństwa państwa w cyberprzestrzeni.	P7S_KK P7S_KR

Organizacja													
Forma zajęć	Wykład (W)	Ćwiczenia w grupach											
		A		K		L		S		P		E	
Liczba godzin	30												

Opis metod prowadzenia zajęć

Wykład problemowy z prezentacją multimedialną. Dyskusja. Praca własna studenta – samodzielne studia i przygotowanie do zaliczenia przedmiotu.

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	
W02												X	
W04												X	
U01								X				X	
U02								X				X	
U06								X				X	

K01												X	
K02												X	

Kryteria oceny	Wykład: pisemne kolokwium zaliczeniowe składające się z pytań zamkniętych i otwartych.

Uwagi	

Treści merytoryczne (wykaz tematów)

1.Terminologia i zarys problemu.
2. Cyberprzestrzeń w teoriach i podejściach badawczych w naukach o bezpieczeństwie.
3. Prawne aspekty ochrony cyberprzestrzeni.
4. Zagrożenia dla bezpieczeństwa państwa w cyberprzestrzeni.
5. Wyzwania, szanse w zakresie cyberbezpieczeństwa.
6. Cyberwojna.
7. Wykorzystanie cyberprzestrzeni w celach militarnych.
8. Cyberdyplomacja a bezpieczeństwo państwa.
9. Ochrona praw i wolności człowieka w dobie Internetu.
10. Ochrona cyberprzestrzeni w wybranych państwach i inicjatywy międzynarodowe.

Wykaz literatury podstawowej

Banasiński C. (red.), Cyberbezpieczeństwo. Zarys wykładu, Warszawa 2018.
Hoffmann T., Wybrane aspekty cyberbezpieczeństwa w Polsce, Poznań 2018.
Kura A., Zagrożenia dla bezpieczeństwa informacyjnego państwa u progu XXI wieku, Stalowa Wola 2016.
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).
Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017–2022.

Wykaz literatury uzupełniającej

M. C. Libicki, Cyberdeterrence and Cyberwar, RAND Corporation, Santa Monica, CA 2009.
Tallinn Manual 2.0. on the International Law Applicable to Cyber Operations.
R. Szpyra., Militarne operacje informacyjne, Warszawa 2003.

Bilans godzinowy zgodny z CNPS (Całkowity Nakład Pracy Studenta)

Ilość godzin w kontakcie z prowadzącymi	Wykład	30
	Konwersatorium (ćwiczenia, laboratorium itd.)	
	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	
	Przygotowanie projektu lub prezentacji na podany temat (praca w grupie)	
	Przygotowanie do egzaminu	25
Ogółem bilans czasu pracy		75
Ilość punktów ECTS w zależności od przyjętego przelicznika		3