

KARTA KURSU

Nazwa	Środowisko cyberbezpieczeństwa
-------	--------------------------------

Koordynator	dr Agnieszka Warchoń	Zespół dydaktyczny: dr Agnieszka Warchoń
-------------	-----------------------------	---

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

Opis kursu (cele kształcenia)

Kurs ma na celu ukazanie cyberprzestrzeni jako współczesnego wymiaru środowiska bezpieczeństwa państwa oraz istotnego obszaru funkcjonowania podmiotów politycznych, społecznych i gospodarczych. Przedmiot koncentruje się na analizie systemowej uwarunkowań cyberbezpieczeństwa, obejmujących aspekty strategiczne, prawne, instytucjonalne i społeczne.

W ramach zajęć omawiane są mechanizmy rywalizacji i współpracy w cyberprzestrzeni, operacje wpływu, zewnętrzne ingerencje w procesy demokratyczne, rola mediów społecznościowych w kształtowaniu środowiska bezpieczeństwa międzynarodowego oraz znaczenie odporności społecznej na zagrożenia informacyjne.

Szczególne uwagi poświęcone jest studiom przypadków, w tym wojnie Rosji z Ukrainą, jako przykładom funkcjonowania środowiska cyberbezpieczeństwa w warunkach konfliktu. Celem przedmiotu jest rozwinięcie u studentów umiejętności analizy zagrożeń i procesów zachodzących w cyberprzestrzeni z perspektywy nauk społecznych, w tym nauk o bezpieczeństwie oraz kształtowanie zdolności krytycznej oceny współczesnych wyzwań dla bezpieczeństwa państwa i społeczeństwa.

Efekty kształcenia

	Efekt kształcenia dla kursu	Odniesienie do efektów kierunkowych
Wiedza	W01: Student zna i rozumie terminologię dotyczącą środowiska cyberbezpieczeństwa i różnego rodzaju uwarunkowania w tym zakresie.	K_W07, K_W08
	W02: Student zna kategorie poznania naukowego, które determinują cyberbezpieczeństwo podmiotu, i rozumie zależności między nimi, oraz ich uwarunkowania.	K_W07
	W03: Student w zaawansowanym stopniu zna i rozumie ogół warunków wewnętrznych i zewnętrznych, militarnych i niemilitarnych funkcjonowania danego podmiotu w cyberprzestrzeni.	K_W07, K_W10

	Efekt kształcenia dla kursu	Odniesienie do efektów kierunkowych
Umiejętności	U01: Student posiada umiejętności wyszukiwania i przetwarzania informacji na temat środowiska cyberbezpieczeństwa, przy użyciu różnych źródeł i zaawansowanych technik informacyjno-komunikacyjnych (ICT), oraz potrafi dokonać ich interpretacji.	K_U11, K_U12
	U02: Student potrafi wskazać przykłady określonych wyzwań, szans, zagrożeń i ryzyk dla cyberbezpieczeństwa państwa, a przez właściwy dobór źródeł oraz informacji z nich pochodzących, dokonywać oceny, krytycznej analizy i syntezy tych informacji.	K_U10
	U03: Student potrafi zastosować wiedzę teoretyczną do analizy środowiska cyberbezpieczeństwa określonego podmiotu.	K_U10, K_U11
	U04: Student potrafi samodzielnie planować własne uczenie się, w tym potrafi aktualizować informacje zdobyte w trakcie kursu, co jest konieczne biorąc pod uwagę specyfikę cyberprzestrzeni i dynamikę zmian w niej zachodzących.	K_U10, K_U12

	Efekt kształcenia dla kursu	Odniesienie do efektów kierunkowych
Kompetencje społeczne	K01: Student ma świadomość ograniczeń własnej wiedzy i umiejętności w zakresie środowiska cyberbezpieczeństwa.	K_K02, K_K04
	K02: Student potrafi pracować samodzielnie z danymi dotyczącymi środowiska cyberbezpieczeństwa danego podmiotu i jest gotów do krytycznej oceny własnych działań z zachowaniem zasad rzetelności naukowej.	K_K02
	K03: Student potrafi pracować (zarówno kierować, jak i uczestniczyć) w grupie w zakresie interpretacji determinantów środowiska cyberbezpieczeństwa, uwarunkowań oraz literatury przedmiotu w tym zakresie, oraz jest gotów wziąć odpowiedzialność za efekty pracy.	K_K01

Organizacja											
Forma zajęć	Wykład (W)	Ćwiczenia w grupach									
		A		K		L		S		P	E
Liczba godzin	30			15							

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				
U04	X					X	X	X	X				
K01	X					X	X		X				
K02	X					X	X		X				
K03	X					X	X		X				

Opis metod prowadzenia zajęć

Kryteria oceny	Audytoryum Na zaliczenie składają się: <ol style="list-style-type: none"> 1. Projekty indywidualne lub grupowe w formie prezentacji i omówienia wybranych tematów. 2. Obecność.
	Wykład Zaliczenie: Pozytywny wynik z testu jednokrotnego wyboru.
Uwagi	Indywidualny program studiów – warunki zaliczenia ustalane indywidualnie z prowadzącym zajęcia po przedstawieniu zgody na indywidualny tok studiów.

Treści merytoryczne (wykaz tematów)

Wykład <ol style="list-style-type: none"> 1. Zajęcia organizacyjne. Przedstawienie warunków zaliczenia przedmiotu. Wstęp do problematyki środowiska cyberbezpieczeństwa. 2. Cyberprzestrzeń jako kategoria analityczna w naukach o bezpieczeństwie. 3. Ontologia i epistemologia cyberprzestrzeni. 4. Środowisko cyberbezpieczeństwa. 5. Cyberprzestrzeń w teorii stosunków międzynarodowych. 6. Cyberoperacje jako instrument polityki bezpieczeństwa. 7. Konflikty hybrydowe i wojna informacyjna. 8. Krajowy system cyberbezpieczeństwa Rzeczypospolitej Polskiej 9. Regionalny i globalny wymiar regulacji cyberprzestrzeni. 10. Społeczne determinanty cyberbezpieczeństwa. 11. Ochrona praw i wolności jednostki w środowisku cyfrowym. 12. Cybersuwerenność i fragmentacja globalnej sieci. 13. Cyberprzestępczość. 14. Cyberataki na infrastrukturę krytyczną.

Audytarium

1. Zajęcia organizacyjne. Przedstawienie warunków zaliczenia zajęć audytoryjnych i wstęp do tematyki.
2. Zewnętrzne ingerencje w procesy wyborcze jako element destabilizacji środowiska cyberbezpieczeństwa państwa – analiza cyklu wyborczego 2024–2025.
3. Media społecznościowe jako strukturalny komponent środowiska cyberbezpieczeństwa międzynarodowego.
4. Cyfrowy populizm i polaryzacja społeczna jako czynniki osłabiające odporność środowiska cyberbezpieczeństwa.
5. Cyberformacje jako element architektury bezpieczeństwa narodowego – analiza porównawcza wybranych państw.
6. Wojna Rosji z Ukrainą jako studium funkcjonowania środowiska cyberbezpieczeństwa w warunkach konfliktu zbrojnego.
7. Prognozowanie rozwoju środowiska cyberbezpieczeństwa w perspektywie konfliktów przyszłości.

Wykaz literatury podstawowej

- 1) Banasiński C. (red.), *Cyberbezpieczeństwo. Zarys wykładu*, Wolters Kluwers, Warszawa 2023.
- 2) Kitler W., Taczkowska-Olszewska J., Radoniewicz F. (red.), *Ustawa o krajowym systemie cyberbezpieczeństwa. Komentarz*, C.H.Beck, Warszawa 2019.
- 3) Lakomy, M., *Cyberprzestrzeń jako nowy wymiar rywalizacji i współpracy państw*, Wydawnictwo Uniwersytetu Śląskiego, Katowice 2015.
- 4) Siudak R., *Cyberbezpieczeństwo w Polsce*, Kraków 2022.
- 5) *Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa* (Dz.U. 2018 poz. 1560).
- 6) Uchwała nr 125 Rady Ministrów z dnia 22 października 2019 r. w sprawie *Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019–2024*

Wykaz literatury uzupełniającej

- 1) Ball M., *Metawersum. Jak internet przyszłości zrewolucjonizuje świat i biznes*, Warszawa 2022.
- 2) Buchanan, Ben, *The Cybersecurity Dilemma: Hacking, Trust and Fear Between Nations*, Oxford University Press, New York 2017.
- 3) Dela R.T., *Założenia działań w cyberprzestrzeni*, Warszawa 2022.
- 4) Galloway S., *Wielka czwórka. Ukryte DNA: Amazon, Apple, Facebook i Google*, Poznań 2018.
- 5) Hoffmann T., *Wybrane aspekty cyberbezpieczeństwa w Polsce*, Poznań 2018.
- 6) Krawiec J., *Cyberbezpieczeństwo. Podejście systemowe*. Oficyna Wydawnicza Politechniki Warszawskiej, Warszawa 2020.
- 7) Kreft J., *Władza platform. Za fasadą Google, Facebooka i Spotify*, Kraków 2021.
- 8) Kura A., *Zagrożenia dla bezpieczeństwa informacyjnego państwa u progu XXI wieku*, Stalowa Wola 2016.
- 9) Lee K-F., *Inteligencja sztuczna, rewolucja prawdziwa. Chiny, USA i przyszłość świata*, Poznań 2018.
- 10) Libicki M.C., *Cyberdeterrence and Cyberwar*, RAND Corporation, Santa Monica, CA 2009.
- 11) Liderman K., *Bezpieczeństwo informacyjne. Nowe wyzwania*, PWN, Warszawa 2017.
- 12) M. Siwicki, *Cyberprzestępczość*, C.H.Beck, Warszawa 2013.
- 13) Marczevska-Rytka M. (red.), *Haktywizm (cyberterroryzm, haking, protest obywatelski, cyberaktywizm, e-mobilizacja)*, Lublin 2014.
- 14) NASK, *Raport roczny z działalności CERT Polska. Krajobraz bezpieczeństwa polskiego internetu*, NASK, Warszawa 2023.
- 15) Olejnik Ł., Kurasiński A., *Filozofia cyberbezpieczeństwa. Jak zmienia się świat? Od złośliwego oprogramowania do cyberwojny*, PWN, Warszawa 2022.
- 16) Perlroth N., *Cyberbroń i wyścig zbrojeń*, Warszawa 2021.
- 17) Rid T., *Wojna informacyjna*, Warszawa 2020.

- 18) *Stanowisko Rzeczypospolitej Polskiej dotyczące zachowania prawa międzynarodowego w cyberprzestrzeni*: <https://www.gov.pl/attachment/8f6b929b-a2b7-4662-beac-d7f4a512b82c>.
- 19) Starzec S., *Krajowa Mapa Cyberbezpieczeństwa*, Instytut Promyka, Warszawa 2022.
- 20) Szpor G., Gryszczyńska A., Czaplicki K., *Ustawa o krajowym systemie cyberbezpieczeństwa. Komentarz*, Wolters Kluwer, Warszawa 2019.
- 21) *The Tallinn Manual 2.0*
- 22) Warchoł A., *Wpływ cyberprzestrzeni na bezpieczeństwo państwa na początku XXI wieku (praca doktorska)*, Kraków 2017(wybrane fragmenty).
- 23) Warchoł A., *Wpływ podmiotów zewnętrznych w cyberprzestrzeni na bezpieczeństwo procesu wyborczego w państwie*, „Polityka i społeczeństwo” 2025, t. 23. Nr 1.
- 24) Warchoł A., *Cybersuwerenność* [w:] *Encyklopedia bezpieczeństwa* pod red. O. Wasiuta, S. Wasiuta, 2025.
- 25) Warchoł A., *The Role of Social Media in Shaping the State Security Environment*, “Security Dimensions. International & National Studies” 2024.
- 26) *Vademecum bezpieczeństwa informacyjnego (wybór haseł)*.
- 27) Zuboff S., *Wiek kapitalizmu inwigilacji. Walka o przyszłość ludzkości na nowej granicy władzy*, Wydawnictwo Zysk i S-ka, Poznań 2020.

Bilans godzinowy zgodny z CNPS (Całkowity Nakład Pracy Studenta)

liczba godzin w kontakcie z prowadzącymi	Wykład	30
	Konwersatorium (ćwiczenia, laboratorium itd.)	15
	Pozostałe godziny kontaktu studenta z prowadzącym	5
liczba godzin pracy studenta bez kontaktu z prowadzącymi	Lektura w ramach przygotowania do zajęć	10
	Przygotowanie projektu lub prezentacji na podany temat (praca indywidualna)	10
	Przygotowanie do egzaminu/zaliczenia	5
Ogółem bilans czasu pracy		75
Liczba punktów ECTS w zależności od przyjętego przelicznika		3