

KARTA KURSU

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

Koordynator	dr Agnieszka Warchoł	Zespół dydaktyczny: dr Agnieszka Warchoł mgr Mateusz Łabuz
-------------	-----------------------------	--

Punktacja ECTS*	Studia stacjonarne: 4
	Studia niestacjonarne:4

Opis kursu (cele kształcenia)

Celem kształcenia jest nabycie przez studentów wiedzy oraz umiejętności dotyczących środowiska cyberbezpieczeństwa. Ponadto, student po ukończeniu kursu posiada kompetencje społeczne w zakresie samodoskonalenia oraz pracy w grupie, a także potrafi krytycznie ocenić posiadaną wiedzę. Tematyka zajęć obejmuje ogół warunków wewnętrznych i zewnętrznych, militarnych i pozamilitarnych funkcjonowania państwa w cyberprzestrzeni. Ponadto, przez pryzmat wyzwań, szans, zagrożeń i ryzyk studenci podejmą próbę określenia misji, wizji oraz celów podmiotu bezpieczeństwa.

Efekty uczenia się

	Efekt uczenia się dla kursu	Odniesienie do efektów kierunkowych
Wiedza	W01: Student w zaawansowanym stopniu 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 uczenia się 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 wykorzystać wiedzę 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 uczenia się dla kursu	Odniesienie do efektów kierunkowych
Kompetencje społeczne	K01: Student ma pogłębiona świadomość poziomu swojej 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.	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

Studia stacjonarne

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

Studia niestacjonarne

		Organizacja										
Forma zajęć	Wykład (W)	Ćwiczenia w grupach										
		A		K		L		S		P		E
Liczba godzin	20			10								

Opis metod prowadzenia zajęć

Ćwiczenia:

1. Zajęcia organizacyjne. Przedstawienie warunków zaliczenia ćwiczeń. Wstęp do cyberbezpieczeństwa.
2. Terminologia, rozróżnienie między cyberprzestrzenią oraz przestrzenią informacyjną.
3. Cyberbezpieczeństwo w przestrzeni międzynarodowej – regulacje ONZ i UE.
4. Cyberbezpieczeństwo RP – uwarunkowania i wyzwania.
5. Krajowy system cyberbezpieczeństwa – regulacje, interesariusze, obowiązki.
6. Podstawowe zagrożenia w cyberprzestrzeni w wymiarze politycznym i społecznym.
7. Najważniejsze formy ataków i podstawy cyberbezpieczeństwa indywidualnego.
8. Cyberbezpieczeństwo jako nowa domena działań militarnych.
9. Współczesne konflikty i militarny wymiar cyberbezpieczeństwa.
10. Bezpieczeństwo przestrzeni informacyjnej - wprowadzenie.
11. Dezinformacja i fake news – zagrożenia dla bezpieczeństwa przestrzeni informacyjnej.
12. Wprowadzenie do sztucznej inteligencji.
13. Sztuczna inteligencja w cyberbezpieczeństwie – szanse i zagrożenia.
14. Prezentacja wniosków i rekomendacji z projektów indywidualnych i grupowych realizowanych przez studentów.
15. Podsumowanie ćwiczeń.

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		x	
W02	x					x	x	x		x		x	
W03	x					x	x	x		x		x	
U01	x					x	x	x		x		x	
U02	x					x	x	x		x		x	
U03	x					x	x	x		x		x	
U04	x					x	x	x		x		x	
K01	x					x	x	x		x		x	
K02	x					x	x	x		x		x	
K03	x					x	x	x		x		x	

Kryteria oceny	<p>Ćwiczenia</p> <p>Projekty indywidualne lub grupowe w formie prezentacji i omówienia wybranych tematów.</p> <p>Wykład</p> <p>Projekt grupowy na wybrany temat kończący się raportem i prezentacją wniosków i rekomendacji.</p> <p>Warunkiem uzyskania oceny z egzaminu jest zaliczenie ćwiczeń.</p>
Uwagi	Indywidualny program studiów – warunki zaliczenia ustalane indywidualnie z prowadzącym zajęcia po przedstawieniu zgody na indywidualny tok studiów.

Treści merytoryczne (wykaz tematów)

Wykład

1. Zajęcia organizacyjne. Przedstawienie warunków zaliczenia przedmiotu.
2. Terminologia, zarys problemu, określenie celu i przedmiotu kursu.
3. Cyberprzestrzeń jako odrębne środowisko i kolejna płaszczyzna funkcjonowania danego podmiotu.
4. Środowisko cyberbezpieczeństwa – próba charakterystyki. Kategorie poznania naukowego, które determinują cyberbezpieczeństwo podmiotu (wyzwania, szanse, zagrożenia, ryzyka).
5. Cyberprzestrzeń jako wymiar współpracy i rywalizacji państw.
6. Ofensywne wykorzystanie cyberprzestrzeni.
7. Polska – krajowy system cyberbezpieczeństwa. Polityka cyberbezpieczeństwa: aspekty prawne, organizacyjne i instytucjonalne.
8. Wybrane regulacje regionalne i międzynarodowe w zakresie cyberbezpieczeństwa. Stosowanie prawa międzynarodowego w cyberprzestrzeni.
9. Społeczne aspekty cyberbezpieczeństwa.
10. Ochrona praw i wolności człowieka w Internecie.
11. Rola mediów społecznościowych w kształtowaniu środowiska cyberbezpieczeństwa.
12. Nowe trendy w cyberbezpieczeństwie.
13. Prezentacja wniosków i rekomendacji z ukończenia projektów przez studentów.
14. Podsumowanie wykładów.

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-Rytko M. (red.), *Haktywizm (cyberterrorizm, 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) Perloth 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) Warchoń A., *Wpływ cyberprzestrzeni na bezpieczeństwo państwa na początku XXI wieku (praca doktorska)*, Kraków 2017 (wybrane fragmenty).
- 23) *Vademecum bezpieczeństwa informacyjnego (wybór haseł)*.
- 24) 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) – studia stacjonarne

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	20
	Przygotowanie projektu lub prezentacji na podany temat (praca indywidualna)	10
	Przygotowanie do egzaminu/zaliczenia	20
Ogółem bilans czasu pracy		100
Liczba punktów ECTS w zależności od przyjętego przelicznika		4

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

liczba godzin w kontakcie z prowadzącymi	Wykład	20
	Konwersatorium (ćwiczenia, laboratorium itd.)	10
	Pozostałe godziny kontaktu studenta z prowadzącym	5
liczba godzin pracy studenta bez kontaktu z prowadzącymi	Lektura w ramach przygotowania do zajęć	25
	Przygotowanie projektu lub prezentacji na podany temat (praca indywidualna)	20
	Przygotowanie do egzaminu/zaliczenia	20
Ogółem bilans czasu pracy		100
Liczba punktów ECTS w zależności od przyjętego przelicznika		4