Załącznik nr 4 do Zarządzenia Nr RD/Z.0201-2/2018

KARTA KURSU

Nazwa	Sztuczna Inteligencja a Bezpieczeństwo
Nazwa w j. ang.	Artificial Intelligence and Security

Kod		Punktacja ECTS*	2

Koordynator	Mgr Mateusz Łabuz	Zespół dydaktyczny: Mgr Mateusz Łabuz

Opis kursu (cele kształcenia)

Celem kształcenia jest nabycie przez studentów wiedzy oraz umiejętności dotyczących rozwoju sztucznej inteligencji (SI) i wyzwań dla bezpieczeństwa związanych z upowszechnieniem technologii. W ramach cyklu audytoriów realizowane są także zagadnienia uzupełniające z zakresu bezpieczeństwa przestrzeni informacyjnej, ze szczególnym uwzględnieniem dezinformacji i deep fakes generowanych z wykorzystaniem SI. Ponadto, student po ukończeniu kursu posiada kompetencje społeczne w zakresie samodoskonalenia, prezentacji i pracy indywidualnej, a także potrafi krytycznie ocenić posiadaną wiedzę. Tematyka zajęć obejmuje ogół warunków wewnętrznych i zewnętrznych, regulacyjnych, etycznych, gospodarczych, biznesowych, militarnych i pozamilitarnych wykorzystywania SI przez organizacje, państwa i jednostki, jak również społecznych i politycznych implikacji rozwoju technologii opartych na SI.

Efekty kształcenia

	Efekt kształcenia dla kursu	Odniesienie do efektów kierunkowych
Wiedza	W01: Student w zaawansowanym stopniu zna i rozumie terminologię dotyczącą sztucznej inteligencji i różnego rodzaju form jej zastosowania.	K1_W03, K1_W04
	W02: Student zna kategorie poznania naukowe, które wpływają na bezpieczeństwo podmiotów w związku z wykorzystaniem sztucznej inteligencji i rozumie zależności między nimi, jak również wyzwania i perspektywy.	K1_W01, K1_W05
	W03: Student w zaawansowanym stopniu zna i rozumie ogół warunków wewnętrznych i zewnętrznych wykorzystania sztucznej inteligencji w różnych sektorach.	K1_W02, K1_W06

	Efekt kształcenia dla kursu	Odniesienie do efektów kierunkowych
Umiejętności	U01: Student posiada umiejętności wyszukiwania i przetwarzania informacji na temat sztucznej inteligencji, przy użyciu różnych źródeł i zaawansowanych technik informacyjno-komunikacyjnych (ICT), oraz potrafi dokonać ich interpretacji.	K1_U01, K1_U04
	U02: Student potrafi wskazać konsekwencje dla środowiska bezpieczeństwa, w tym szanse i ryzyka, związane z rozwojem sztucznej inteligencji i jej wykorzystaniem w różnych sektorach.	K1_U02, K1_U03
	U03: Student potrafi dokonać krytycznej analizy źródeł, uzupełniać wiedzę oraz wykorzystać ją do bieżącej i ukierunkowanej na przyszłość analizy środowiska bezpieczeństwa w kontekście wykorzystania sztucznej inteligencji.	K1_U01, K1_U04
	U04: Student potrafi samodzielnie planować własne uczenie się oraz przygotować materiały do prezentacji indywidualnej i dyskusji.	K1_U05

	Efekt kształcenia dla kursu	Odniesienie do efektów kierunkowych
Kompetencje społeczne	K01: Student ma świadomość poziomu swojej wiedzy i umiejętności w zakresie oceny środowiska bezpieczeństwa w kontekście wykorzystania sztucznej inteligencji.	K_K01, K_K02
	K02: Student potrafi pracować samodzielnie z danymi dotyczącymi sztucznej inteligencji oraz krytycznie ewaluować materiały.	K_K01
	K03: Student potrafi pracować indywidualnie oraz w grupie w zakresie prezentacji i ewaluacji materiałów dotyczących wpływu sztucznej inteligencji na środowisko bezpieczeństwa i procesy społeczne, w tym wykorzystać zdobytą wiedzę w praktyce do działań na rzecz społeczeństwa i państwa.	K_K01, K_K03 K_K04
	K04: Student jest gotów wziąć odpowiedzialność za efekty swojej pracy oraz przedstawić wyniki badań na forum grupy i wziąć udział w dyskusji.	

Organizacja		
Forma zajęć	Wykład	Ćwiczenia w grupach

	(W)	A	K	L	S	P	E
Liczba godzin		30					

Opis metod prowadzenia zajęć

Audytorium: wykład w formie dyskusji ze studentami oraz ewaluacja projektów indywidualnych prezentowanych przez studentów na forum grupy (wraz z dyskusją, krytyczną ewaluacją oraz symulacją obrony przygotowanego materiału).

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	X				
K02	X					X	X	X	X				
K03	X					X	X	X	X				
K04	X					X	X	X	X				

Kryteria oceny	Projekty indywidualne w formie prezentacji i omówienia wybranych tematów, w tym dyskusji na forum grupy.

Uwagi	Indywidualny program studiów – warunki zaliczenia ustalane indywidualnie z prowadzącym zajęcia po przedstawieniu zgody na indywidualny tok studiów.

Treści merytoryczne (wykaz tematów)

Audytorium:

1. Wprowadzenie do sztucznej inteligencji (SI)
2. Regulacje prawne dot. środowiska SI
3. Unijny Akt o Sztucznej Inteligencji i jego implikacje
4. Etyka sztucznej inteligencji – czym jest SI godna zaufania?
5. Cyberbezpieczeństwo a SI
6. Militarne wykorzystanie SI
7. Bezpieczeństwo przestrzeni informacyjnej a SI
8. Deep fakes jako szczególne zagrożenie dla środowiska informacyjnego
9. Ochrona danych i prywatności a SI
10. Wpływ SI na rynek pracy i procesy społeczne
11. SI w wybranych sektorach gospodarki, cz. 1
12. SI w wybranych sektorach gospodarki, cz. 2
13. Globalne trendy i wyzwania związane z rozwojem SI
14. Podsumowanie wykładów
15. Prezentacje indywidualne dot. różnych aspektów wykorzystania SI

Wykaz literatury podstawowej

1) Ball M., *Metawersum. Jak internet przyszłości zrewolucjonizuje świat i biznes.*
2) Crawford K., *Atlas sztucznej inteligencji*
3) Harari Y. N., *21 lekcji na XXI wiek*
4) Huttenlocher D., Kissinger H., *Era sztucznej inteligencji*
5) Kura A., *Zagrożenia dla bezpieczeństwa informacyjnego państwa u progu XXI wieku.*
6) Kurp F., *Sztuczna inteligencja od podstaw*
7) Kwartalnik Więź, *Ludzie vs. sztuczna inteligencja*, wyd. lato 2023
8) Lee K-F., *Inteligencja sztuczna, rewolucja prawdziwa. Chiny, USA i przyszłość świata.*
9) Lennox J. C., *2084. Sztuczna inteligencja i przyszłość ludzkości*
10) Miesięcznik Znak, *Pokolenie sztucznej inteligencji*, wyd. marzec 2024
11) Przegalińska A., Jemielniak D., *AI w strategii: rewolucja sztucznej inteligencji w zarządzaniu*
12) Przegalińska A., *Sztuczna inteligencja. Nieludzka, arcyludzka*
13) Strittmatter K., *Chiny 5.0. Jak powstaje cyfrowa dyktatura*
14) Tegmark M., *Życie 3.0. Człowiek w erze sztucznej inteligencji*

Wykaz literatury uzupełniającej

1) Banasiński C. (red.), *Cyberbezpieczeństwo. Zarys wykładu*
2) Böswald L. M., Saab B. A., *What a Pixel Can Tell: Text-to-Image Generation and its Disinformation Potential*
3) Fallis D., *The Epistemic Threat of Deepfakes*
4) Farid H., *Creating, Using, Misusing, and Detecting Deep Fakes*
5) Habgood-Coote J., *Deepfakes and the epistemic apocalypse*
6) Hoffmann T., *Wybrane aspekty cyberbezpieczeństwa w Polsce*
7) Krawiec J., *Cyberbezpieczeństwo. Podejście systemowe*
8) Laux J., Wachter S., Mittelstadt B., *Trustworthy artificial intelligence and the European Union AI act: On the conflation of trustworthiness and acceptability of risk*
9) Łabuz M., *Regulating Deep Fakes in the Artificial Intelligence Act*
10) Mahler T., *Between risk management and proportionality: The risk-based approach in the EU's Artificial Intelligence Act Proposal*
11) Mustak M. i in., *Deepfakes: Deceptions, mitigations, and opportunities*
12) NASK, *Raport roczny z działalności CERT Polska. Krajobraz bezpieczeństwa polskiego internetu*
13) Okolie C., *Artificial Intelligence-Altered Videos (Deepfakes), Image-Based Sexual Abuse, and Data Privacy Concerns*
14) Rigotti C., McGlynn C., *Towards an EU criminal law on violence against women: The*

ambitions and limitations of the Commission's proposal to criminalise image-based sexual abuse
15) Smuha N. A., *Beyond the Individual: Governing AI's Societal Harm*
16) Wasiuta O., Klepka R. (red.) *Vademecum bezpieczeństwa informacyjnego* (wybór haseł)

Bilans godzinowy zgodny z CNPS (Całkowity Nakład Pracy Studenta)

Ilość godzin w kontakcie z prowadzącymi	Wykład	0
	Konwersatorium (ćwiczenia, laboratorium itd.)	30
	Pozostałe godziny kontaktu studenta z prowadzącym	5
Ilość godzin pracy studenta bez kontaktu z prowadzącymi	Lektura w ramach przygotowania do zajęć	5
	Przygotowanie krótkiej pracy pisemnej lub referatu po zapoznaniu się z niezbędną literaturą przedmiotu	5
	Przygotowanie projektu lub prezentacji na podany temat (praca w grupie)	5
	Przygotowanie do egzaminu/zaliczenia	0
Ogółem bilans czasu pracy		50
Ilość punktów ECTS w zależności od przyjętego przelicznika		2