Załącznik nr 4 do Zarządzenia Nr……..

KARTA KURSU

Nazwa	Cyberbezpieczeństwo
Nazwa w j. ang.	Cybersecurity

Koordynator	dr Paulina Motylińska	Zespół dydaktyczny
		dr Paulina Motylińska
Punktacja ECTS*	1	

Opis kursu (cele kształcenia)

- Celem kursu jest zapoznanie studentów z podstawowymi zagadnieniami związanymi z cyberbezpieczeństwem. Studenci poznają podstawowe pojęcia w zakresie cyberbezpieczeństwa (m.in. cyberbezpieczeństwo, cyberprzestrzeń, cyberprzestępczość, bezpieczeństwo informacji). Tematyka zajęć obejmuje treści związane z cyberbezpieczeństwem różnych podmiotów (państwa, organizacji i jednostki). Przedstawione zostanie także szerokie rozumienie zjawiska cyberprzestępczości (w ujęciu Konwencji Rady Europy o Cyberprzestępczości) jako przestępstw przeciwko poufności, integralności i dostępności danych informatycznych i systemów, przestępstw tzw. komputerowe, przestępstw ze względu na charakter zawartych informacji oraz przestępstw związane z naruszeniem praw autorskich i praw pokrewnych.

Warunki wstępne

Wiedza	-
Umiejętności	-
Kursy	-

Efekty kształcenia

	Efekt kształcenia dla kursu	Odniesienie do efektów kierunkowych
Wiedza	W01: Student zna znaczenie i relacje pomiędzy podstawowymi pojęciami związanymi z cyberbezpieczeństwem (np. cyberprzestrzeń, cyberprzestępczość, cyberzagrożenia, bezpieczeństwo informacji). W02: Student zna podstawowe regulacje prawne i organizacyjne związane z zachowaniem cyberbezpieczeństwa państwa, organizacji i jednostki. W03: Student zna typy cyberzagrożeń i cyberprzestępstw oraz wskazuje możliwości przeciwdziałania im i ich zwalczania.	K2_W01 K2_W06

	Efekt kształcenia dla kursu	Odniesienie do efektów kierunkowych
Umiejętności	U01: Student potrafi wykorzystać wiedzę teoretyczną do analizy i charakterystyki wybranych typów cyberzagrożeń. U02: Student potrafi w sposób prawidłowy posługiwać się nomenklaturą pojęciową w tematyce cyberbezpieczeństwa.	K2_U04 K2_U02

	Efekt kształcenia dla kursu	Odniesienie do efektów kierunkowych
Kompetencje społeczne	K01: Student samodzielnie rozszerza swoją wiedzę w zakresie cyberbezpieczeństwa. K02. Student rozumie znaczenie zachowania cyberbezpieczeństwa we współczesnym świecie.	K2_K02 K2_K01

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

Opis metod prowadzenia zajęć

- Wykład z wykorzystaniem prezentacji multimedialnych i filmów. Każde zajęcia kończą się quizem podsumowującym i sprawdzającym wiedzę studentów.
- Część zajęć może zostać poprowadzona w sposób aktywizujący studentów (dyskusja na zadany temat).

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	Kolokwium pisemne	Inne
W01												x	
W02												x	
W03												x	
U01								x				x	
U02								x				x	
K01								x				x	
K02								x					

Kryteria oceny	Zaliczenie na podstawie: - obecności (wymagane minimum 80% obecności) - aktywności na zajęciach (udział w quizie) - pozytywnego wyniku z kolokwium kończącego zajęcia (uzyskanie minimum 60% poprawnych odpowiedzi)

Uwagi	-

Treści merytoryczne (wykaz tematów)

1. Wstęp: cyberprzestrzeń, cyberbezpieczeństwo, cyberzagrożenia, cyberprzestępczość, bezpieczeństwo informacyjne, bezpieczeństwo informacji
2. Cyberbezpieczeństwo państwa – formy zagrożeń (m.in. haktywizm, cyberprzestępczość, cyberterroryzm, cyberwojna)
3. Europejski i krajowy system cyberbezpieczeństwa, Strategia Cyberbezpieczeństwa RP
4. Cyberbezpieczeństwo z perspektywy firmy/organizacji – SZBI, audyt bezpieczeństwa, normy
5. Cyberbezpieczeństwo dzieci i młodzieży (pedofilia i pornografia w Internecie, kompetencje informacyjne i cyfrowe)
6. Cyberprzestępczość – podział cyberprzestępstw według Konwencji Rady Europy o Cyberprzestępczości

Wykaz literatury podstawowej

1. Red. Banasiński C. (2018). *Cyberbezpieczeństwo: zarys wykła*du. Warszawa: Wolters Kluwer.
2. Red. Banasiński C., Rojszczak M. (2020). *Cyberbezpieczeństwo*. Warszawa: Wolters Kluwer.
3. Lakomy, M. (2015). *Cyberprzestrzeń jako nowy wymiar rywalizacji i współpracy państw*. Katowice: Wydawnictwo UŚ.
4. Liderman K. (2017). *Bezpieczeństwo informacyjne. Nowe wyzwania*. Warszawa: PWN. (lub ew. wydanie z 2012)
5. Red. Molendowska M., Miernik R. (2020). *Bezpieczeństwo w cyberprzestrzeni: wybrane zagadnienia*. Toruń: Wydawnictwo Adam Marszałek.
6. Kosiński J. (2015). *Paradygmaty cyberprzestępczości*. Warszawa: Difin.
7. Barlińska J., Małecka A., Świątkowska J. (2018). *Cyberbezpieczeństwo: charakterystyka, mechanizmy i strategie zaradcze w makro i mikro skali*. Warszawa: Texter.
8. Vademecum bezpieczeństwa informacyjnego (wybór haseł) lub Encyklopedia bezpieczeństwa (wybór haseł)

Wykaz literatury uzupełniającej

1. Dębowski T. (2018). *Cyberbezpieczeństwo wyzwaniem XXI wieku*. Łódź-Wrocław: Wydawnictwo Naukowe ArchaeGrapgh.
2. Kowalewski, J.; Kowalewski, M. (2017). *Zagrożenia informacji w cyberprzestrzeni, cyberterroryzm*. Warszawa: Oficyna Wydawnicza Politechniki Warszawskiej.
3. Białkowski, M. (2016). *Ocena prawna i kryminalistyczna przestępczości komputerowej*. Warszawa: CeDeWu.
4. Mitnick K. (2017). *Niewidzialny w sieci. Sztuka zacierania śladów*. Bielsko-Biała: Pascal.

Dodatkowa literatura będzie także podawana na zajęciach.

Bilans godzinowy zgodny z CNPS (Całkowity Nakład Pracy Studenta)

liczba godzin w kontakcie z prowadzącymi	Wykład	10
	Konwersatorium (ćwiczenia, laboratorium itd.)	-
	Pozostałe godziny kontaktu studenta z prowadzącym	-
liczba 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	-
	Przygotowanie projektu lub prezentacji na podany temat (praca w grupie)	-
	Przygotowanie do egzaminu/zaliczenia	10
Ogółem bilans czasu pracy		25
Liczba punktów ECTS w zależności od przyjętego przelicznika		1