WYŻSZA SZKOŁA INFORMATYKI STOSOWANEJ I ZARZĄDZANIA WIT
POD AUSPICJAMI POLSKIEJ AKADEMII NAUK
01-447 Warszawa \ ul. Newelska 6 \ www.WIT.edu.pl

WYDZIAŁ INFORMATYCZNYCH TECHNIK ZARZĄDZANIA

Kierunek studiów	Zarządzanie
Profil	Praktyczny
Stopień studiów	1-go stopnia
Forma studiów	niestacjonarne

Sylabus przedmiotu

Bezpieczeństwo w cyberprzestrzeni

1. Dane podstawowe

Status programowy przedmiotu	Blok A: Organizacja i zarządzanie
Rodzaj przedmiotu	Obligatoryjny
Kod przedmiotu	LZN-BWC-ZR
Rok studiów	2
Semestr	4
Osoba odpowiedzialna za przedmiot	dr Andrzej Kozłowski
Język wykładowy	polski

2. Wymiar godzin i forma zajęć

Rodzaj	Liczba godzin
Wykład	16
Projekt	8
Razem godzin	24

3. Cele przedmiotu

Kod	Cel
CP1	Zdobycie wiedzy dotyczącej podstawowych zagrożeń w cyberprzestrzeni oraz środków, które pozwalają na ochronę przed nimi.
CP2	Zdobycie umiejętności pozwalających na bezpieczne użytkowanie cyberprzestrzeni
CP3	Studenci zdobywają odpowiednie kompetencje społeczne przygotowujące do uczestnictwa w projektach z zakresu cyberbezpieczeństwa.

4. Wymagania wstępne w zakresie wiedzy, umiejętności i innych kompetencji

Podstawowa wiedza z zakresu bezpieczeństwa oraz informatyki

5. Efekty uczenia się

Wiedza

Kod	Student zna i rozumie:	Realizuje cel	Efekty kierunkowe
EU-W1	Studenci mają poszerzoną wiedzę o różnego rodzaju zagrożeniach w cyberprzestrzeni dla pojedyńczych osób, firm oraz infrastruktury krytycznej i państwa	CP1	K1P_W09, K1P_W13, K1P_W22, K1P_W30
EU-W2	Studenci posiadają pogłębioną wiedzę o podstawowych sposobach zabezpieczania się przed zagrożeniami w cyberprzestrzeni	CP1	K1P_W09, K1P_W13, K1P_W22
EU-W3	Studenci posiadają pogłębioną wiedzę o systemie cyberbezpieczeństwa w Polsce i Unii Europejskiej	CP1	K1P_W09, K1P_W13, K1P_W22, K1P_W30
EU-W4	Studenci posiadają pogłębioną wiedzę na temat cyberprzestępczości w Polsce i na świecie	CP1	K1P_W09, K1P_W13, K1P_W22, K1P_W30

Umiejętności

Kod	Student potrafi:	Realizuje cel	Efekty kierunkowe
EU-U1	Studenci potrafią prawidłowo zidentyfikować główne zagrożenia w cyberprzestrzeni takie jak np. phising, ataki DDoS, ransomare czy różnego rodzaju fraudy	CP2	K1P_U07, K1P_U18, K1P_U21, K1P_U29
EU-U2	Studenci samodzielnie identyfikują istotne problemy analityczne polskiego i europejskiego systemu cyberbezpieczeństwa, proponują w tym zakresie przeprowadzenie odpowiednich rozstrzygnięć oraz odpowiednich procedur	CP2	K1P_U07, K1P_U18, K1P_U21, K1P_U29
EU-U3	Studenci wykorzystują zdobytą wiedzę w różnych zakresach i formach, rozszerzoną o krytyczną analizę skuteczności i przydatności stosowania wiedzy	CP2	K1P_U07, K1P_U18, K1P_U21, K1P_U29
EU-U4	Studenci potrafią prawidłowo badać i interpretować zjawiska (polityczne, prawne i ekonomiczne) zachodzące w cyberprzestrzeni i wpływające na cyberbezpieczeństwo	CP2	K1P_U07, K1P_U18, K1P_U21, K1P_U29

Kompetencje

Kod	Student jest gotów do:	Realizuje cel	Efekty kierunkowe
EU-K1	Studenci są gotowi do podejmowana wyzwań ze świadomością znaczenia wiedzy dla rozwiązywania problemów poznawczych i praktycznych	CP3	K1P_K01, K1P_K08, K1P_K10
EU-K2	Studenci są gotowi do krytycznej oceny wiedzy i umiejętności własnych i pochodzących z innych źródeł oraz, na tej podstawie, formułowania potrzeb i zadań poznawczych i praktycznych	CP3	K1P_K01, K1P_K08, K1P_K10
EU-K3	Studenci są zdolni do krytycznego i prawidłowego określenia priorytetów służących realizacji określonego przez siebie lub innych zadań	CP3	K1P_K01, K1P_K08, K1P_K10

6. Treści programowe

Kod	Tematyka	wykład	projekt	Realizuje efekt
TP1	Podstawy działania współczesnego Internetu. Cechy charakterystyczne cyberprzestrzeni	2	0	EU-K1, EU-K2, EU-U1, EU-U2, EU-U3, EU-U4, EU-W1, EU-W2
TP2	Główne rodzaje zagrożeń dla użytkowników, biznesu i instytucji państwowych	1	0	EU-K1, EU-K2, EU-K3, EU-U1, EU-U2, EU-U3, EU-W1, EU-W2
TP3	Dezinformacja i propaganda w Internecie	1	0	EU-K1, EU-K2, EU-K3, EU-U3, EU-U4, EU-W2
TP4	Cyberterroryzm, cyberszpiegostwo, wojna w cyberprzestrzeni	2	0	EU-K1, EU-K2, EU-K3, EU-U1, EU-U4, EU-W3, EU-W4
TP5	Siły zbrojne w cyberprzestrzeni	2	0	EU-K1, EU-K2, EU-K3, EU-U2, EU-U4, EU-W1, EU-W3
TP6	Unia Europejska w cyberprzestrzeni	2	0	EU-K1, EU-K2, EU-K3, EU-U2, EU-W3
TP7	Polski system cyberbezpieczeństwa	2	0	EU-K1, EU-K2, EU-K3, EU-U2, EU-U3, EU-W2, EU-W3
TP8	Geopolityka i prawo międzynarodowe w cyberprzestrzeni	1	0	EU-K1, EU-K2, EU-K3, EU-U2, EU-U3, EU-U4, EU-W3, EU-W4
TP9	Stany Zjednoczone, Rosja, Chin	1	0	EU-K1, EU-K2, EU-K3, EU-U2, EU-U4, EU-W1, EU-W3

Kod	Tematyka	wykład	projekt	Realizuje efekt
TP10	Przyszłość cyberbezpieczeństwa: 5G, Internet rzeczy i sztuczna inteligencja	2	0	EU-K1, EU-K2, EU-K3, EU-U1, EU-W1, EU-W2
TP11	Projekt	0	8	EU-K1, EU-K2, EU-K3, EU-U1, EU-U2, EU-U3, EU-U4, EU-W1, EU-W2, EU-W3, EU-W4

Razem godzin: 24

7. Metody kształcenia

Kod	Metoda
MK1	Wykład z wykorzystaniem prezentacji komputerowej, rzutnika
MK2	Podręczniki i inne materiały dydaktyczne wysyłane studentom

8. Nakład pracy studenta

Aktywność studenta	Obciążenie
Przygotowanie do projektu	46
Przygotowanie do zaliczenia	30
Praca związana z: projekt	8
Praca z nauczycielem związana z: wykład	16
Liczba punktów ECTS (1 punkt=25h)	4
Procentowy udział pracy własnej studenta w sumarycznym obciążeniu studenta	76,00%
Sumaryczne obciążenie pracą studenta	100

9. Status zaliczenia przedmiotu

Studenci przygotowali swoje projekty, który przedstawiali na zajęciach w formie ustnej

Forma studiów	Egzamin	Praca egzaminacyjna	Zaliczenie	Praca zaliczeniowa
niestacjonarne			×	

10. Metody weryfikacji efektów uczenia się

Składowe oceny końcowej

Forma sprawdzenia	Wybrana forma	Punktacja	Realizuje efekt
Egzamin pisemny			
Egzamin ustny			
Sprawdzian pisemny			
Zaliczeniowy przegląd prac			
Referat pisemny			
Referat ustny			
Kolokwium			
Praca domowa			
Miniprojekt			
Praca na zajęciach			
Projekt z dokumentacją			
Ustna prezentacja projektu	×	90	EU-W1, EU-W2, EU-W3, EU-W4, EU-U1, EU-U2, EU-U3, EU-U4, EU-K1, EU-K2, EU-K3
Obecność na zajęciach			
Sprawdzian ustny			
Kartkówka			
Aktywność na zajęciach	×	10	EU-W1, EU-W2, EU-W3, EU-W4, EU-U1, EU-U2, EU-U3, EU-U4, EU-K1, EU-K2, EU-K3
Egzaminacyjny przegląd prac			
Sprawozdanie z praktyki zawodowej			
Prezentacja indywidualna			
Prezentacja zespołowa			

Zasady wyliczania oceny z przedmiotu

Zakres punktów	Ocena
0 – 50	2,0
51 – 60	3,0
61 – 70	3,5
71 – 80	4,0
81 – 90	4,5
91 – 100	5,0

11. Macierz realizacji przedmiotu

Efekt uczenia się	Cel przedmiotu	Treści programowe	Metody kształcenia
EU-W1	CP1	TP1, TP2, TP5, TP9, TP10, TP11	MK1, MK2
EU-W2	CP1	TP1, TP2, TP3, TP7, TP10, TP11	MK1, MK2
EU-W3	CP1	TP4, TP5, TP6, TP7, TP8, TP9, TP11	MK1, MK2
EU-W4	CP1	TP4, TP8, TP11	MK1, MK2
EU-U1	CP2	TP1, TP2, TP4, TP10, TP11	MK1, MK2
EU-U2	CP2	TP1, TP2, TP5, TP6, TP7, TP8, TP9, TP11	MK1, MK2
EU-U3	CP2	TP1, TP2, TP3, TP7, TP8, TP11	MK1, MK2
EU-U4	CP2	TP1, TP3, TP4, TP5, TP8, TP9, TP11	MK1, MK2
EU-K1	CP3	TP1, TP2, TP3, TP4, TP5, TP6, TP7, TP8, TP9, TP10, TP11	MK1, MK2
EU-K2	CP3	TP1, TP2, TP3, TP4, TP5, TP6, TP7, TP8, TP9, TP10, TP11	MK1, MK2
EU-K3	CP3	TP2, TP3, TP4, TP5, TP6, TP7, TP8, TP9, TP10, TP11	MK1, MK2

12. Odniesienie efektów uczenia się

Efekt uczenia się	Efekty kształcenia dla kierunku studiów	Charakterystyki drugiego stopnia w obszarze kształcenia

Efekt uczenia się	Efekty kształcenia dla kierunku studiów	Charakterystyki drugiego stopnia w obszarze kształcenia
EU-W1	K1P_W30, K1P_W22, K1P_W13, K1P_W09	P6S_WG, P6S_WK
EU-W2	K1P_W22, K1P_W13, K1P_W09	P6S_WG, P6S_WK
EU-W3	K1P_W30, K1P_W22, K1P_W13, K1P_W09	P6S_WG, P6S_WK
EU-W4	K1P_W30, K1P_W22, K1P_W13, K1P_W09	P6S_WG, P6S_WK
EU-U1	K1P_U29, K1P_U21, K1P_U18, K1P_U07	P6S_UK, P6S_UW
EU-U2	K1P_U29, K1P_U21, K1P_U18, K1P_U07	P6S_UK, P6S_UW
EU-U3	K1P_U29, K1P_U21, K1P_U18, K1P_U07	P6S_UK, P6S_UW
EU-U4	K1P_U29, K1P_U21, K1P_U18, K1P_U07	P6S_UK, P6S_UW
EU-K1	K1P_K10, K1P_K08, K1P_K01	P6S_KK
EU-K2	K1P_K10, K1P_K08, K1P_K01	P6S_KK
EU-K3	K1P_K10, K1P_K08, K1P_K01	P6S_KK

13. Literatura

Literatura podstawowa

1. Cyberterroryzm zagrożeniem XXI wieku. Perspektywa politologiczna i prawna, Difin, Warszawa 2013
2. Krzysztof Liderman , Bezpieczeństwo informacyjne, Warszawa 2016
3. Tomasz Aleksandrowicz, Świat w sieci. Państwa, społeczeństwa, ludzie. W poszukiwaniu nowego paradygmatu bezpieczeństwa narodowego, Warszawa 2014

Literatura uzupełniająca

1. Marek Górka, Cyberbezpieczeństwo jak podstawa bezpiecznego państwa i społeczeństwa w XXI wieku, Warszawa 2014

Strony WWW

1. https://www.cyberdefence24.pl/
2. https://niebezpiecznik.pl/

14. Informacje o nauczycielach akademickich

Osoby odpowiedzialne za przedmiot

1. dr Andrzej Kozłowski

Osoby prowądzace przedmiot

1. dr Andrzej Kozłowski