SYLABUS PRZEDMIOTU

Polityka cyberbezpieczeństwa

I. Informacje ogólne

Nazwa przedmiotu	*Polityka cyberbezpieczeństwa*
Kod przedmiotu	POC
Rodzaj przedmiotu:	fakultatywny
Kierunek studiów:	Informatyka
Poziom kształcenia:	studia II stopnia
Profil kształcenia:	ogólno-akademicki
Rok studiów:	II
Rodzaje zajęć i liczba godzin	
Wykład	0
Ćwiczenia	15
Laboratoria	0
Praktyki	0
Liczba punktów ECTS	1.5

Imię, nazwisko, tytuł/stopień naukowy, adres e-mail wykładowcy (wykładowców)/ prowadzących zajęcia

- prof. Sebastian Wojciechowski, swoj@amu.edu.pl

Język wykładowy	polski
Przedmiot prowadzony zdalnie (e-learning)	całościowo lub częściowo

II. Informacje szczegółowe

1. Cele przedmiotu

Przedmiot stawia następujące cele:

- poznanie źródeł, tendencji oraz znaczenia rewolucji informatycznej

- nabycie umiejętności identyfikowania i charakteryzowania kluczowych wyzwań oraz zagrożeń dotyczących cyberbezpieczeństwa

- zdobycie wiedzy dotyczącej „miękkich" oraz „twardych" zagrożeń z zakresu cyberbezpieczeństwa

- zdobycie wiedzy z zakresu zwalczania i prognozowania cyberzagrożeń

2. Wymagania wstępne w zakresie wiedzy, umiejętności oraz kompetencji społecznych

Brak

3. Efekty uczenia się (EU) dla zajęć i odniesienie do efektów uczenia się (EK) dla kierunku studiów

Symbol EU dla przedmiotu	Symbol EK dla kierunku studiów	Po zakończeniu modułu i potwierdzeniu osiągnięcia EU student/ka:
POC_01	KINF2_W03 KINF2_U07 KINF2_K01	Zna podstawowe pojęcia oraz zjawiska z zakresu bezpieczeństwa i cyberbezpieczeństwa. Potrafi wskazać cechy cyberprzestrzeni.
POC_02	KINF2_W06 KINF2_U11 KINF2_K02	Potrafi wskazać przyczyny, przejawy oraz następstwa rewolucji informatycznej. Rozumie ich kontekst społeczny oraz technologiczny, a także powiązania ze sferą bezpieczeństwa.
POC_03	KINF2_W06 KINF2_U07 KINF2_K01	Zna „miękkie" wyzwania i zagrożenia dla polityki cyberbezpieczeństwa. Potrafi wytłumaczyć formy i przykłady ich stosowania.
POC_04	KINF2_W06 KINF2_U12 KINF2_K06	Rozumie istotę „twardych" wyzwań i zagrożeń dla polityki bezpieczeństwa. Potrafi scharakteryzować ich przykłady, w tym wskazać znaczenie czy następstwa.
POC_05	KINF2_W06 KINF2_U07 KINF2_K01	Zna formy i metody zwalczania cyberzagrożeń. Potrafi ocenić ich skuteczność wskazując mocne i słabe strony. Umie prognozować nowe potencjalne zagrożenia.

4. Treści programowe zapewniające uzyskanie efektów uczenia się (EU) z odniesieniem do odpowiednich efektów uczenia się (EU) dla przedmiotu

Lp.	Symbol EU dla przedmiotu	Godzin Wykład	Godzin ĆW/ LAB/ SEM	Godzin pracy własnej	Opis treści kształcenia modułu zajęć/przedmiotu
Suma		0	15	20	
1.	POC_01		1	2	Wprowadzenie do polityki bezpieczeństwa i cyberbezpieczeństwa.
2.	POC_02		2	4	Rewolucja informatyczna i główne jej tendencje.
3.	POC_03		4	4	„Miękkie" zagrożenia i wyzwania dla polityki cyberbezpieczeństwa (np. cyfrowa przepaść, cyberszpiegostwo, hacking itp.).
4.	POC_04		4	4	„Twarde" zagrożenia i wyzwania dla polityki cyberbezpieczeństwa (np. cyberwojny, cyberterroryzm itp.).
5.	POC_05		4	6	Zwalczanie cyberzagrożeń oraz prognoza ich przyszłej ewolucji

5. Zalecana literatura

M. Lakomy, Cyberprzestrzeń jako nowy wymiar rywalizacji i współpracy państw, Katowice 2018.

A. Podraza, P. Potakowski, K. Wiak (red.), Cyberterroryzm zagrożeniem XXI wieku. Perspektywa politologiczna i prawna, Warszawa 2015.

M. Siwicki, Cyberprzestępczość, Warszawa 2017.

P. Williams, M. McDonald (eds.), Security Studies, An Introduction, London – New York 2018.

„CyberPolicy Review" Biuletyn PIB NASK, ISSN 2657-8360.

M. Castells, Społeczeństwo sieci, Warszawa 2015.

III. Informacje dodatkowe

1. Metody i formy prowadzenia zajęć umożliwiające osiągnięcie założonych EU (proszę wskazać z proponowanych metod właściwe dla opisywanych zajęć lub/i zaproponować inne)

Realizacja	Metody i formy prowadzenia zajęć
✔	Wykład z prezentacją multimedialną wybranych zagadnień
	Wykład konwersatoryjny
	Wykład problemowy
✔	Dyskusja
	Praca z tekstem
✔	Metoda analizy przypadków
	Uczenie problemowe (Problem-based learning)
	Gra dydaktyczna/symulacyjna
	Rozwiązywanie zadań (np.: obliczeniowych, artystycznych, praktycznych)
	Metoda ćwiczeniowa
	Metoda laboratoryjna

	Metoda badawcza (dociekania naukowego)
	Metoda warsztatowa
	Metoda projektu
	Pokaz I obserwacja
	Demonstracje dźwiękowe i/lub video
	Metody aktywizujące (np.: „burza mózgów", technika analizy SWOT, technika drzewka decyzyjnego, metoda „kuli śniegowej", konstruowanie „map myśli")
	Praca w grupach
✔	Wykład zdalny w czasie rzeczywistym
	Wykład zdalny asynchroniczny uzupełniony spotkaniem w czasie rzeczywistym
	Wykład zdalny asynchroniczny z aktywnością studenta uzupełniony spotkaniem w czasie rzeczywistym
	Ćwiczenia/laboratoria/konwersatoria zdalne w czasie rzeczywistym
	Ćwiczenia zdalne asynchroniczne z pracą indywidualną studenta uzupełnione spotkaniem w czasie rzeczywistym
	Ćwiczenia zdalne asynchroniczne z pracą grupową studentów uzupełnione spotkaniem w czasie rzeczywistym
	Laboratorium cyfrowe zdalne uzupełnione spotkaniem w czasie rzeczywistym
	Konwersatorium asynchroniczne zdalne uzupełnione spotkaniem w czasie rzeczywistym
	Seminarium zdalne w czasie rzeczywistym
	Seminarium asynchroniczne zdalne ze spotkaniem w czasie rzeczywistym
	Inne (jakie?) -

2. Sposoby oceniania stopnia osiągnięcia EU (proszę wskazać z proponowanych sposobów właściwe dla danego EU lub/i zaproponować inne

Sposoby oceniania	Symbole EU dla modułuzajęć/przedmiotu									
	PO C: 01, 02, 03, 04	PO C: 05								
Egzamin pisemny										
Egzamin ustny										
Egzamin z „otwartą książką”										
Kolokwium pisemne										
Kolokwium ustne										
Test										
Projekt										
Esej		✔								
Raport										
Prezentacja multimedialna										
Egzamin praktyczny (obserwacja wykonawstwa)										
Portfolio										
Zadania cząstkowe na wykładzie	✔									
…										


Fundusze
Europejskie
Polska Cyfrowa
Rzeczpospolita
Polska
Unia Europejska
Europejski Fundusz
Rozwoju Regionalnego

3. Nakład pracy studenta i punkty ECTS

Forma aktywności		Średnia liczba godzin na zrealizowanie aktywności
Godziny zajęć (wg planu studiów) z nauczycielem		15
Praca własna studenta*	Przygotowanie do zajęć	
	Czytanie wskazanej literatury	10
	Przygotowanie pracy pisemnej, raportu, prezentacji, itp.	10
	Przygotowanie projektu	
	Przygotowanie pracy semestralnej	
	Przygotowanie do egzaminu/zaliczenia	
	Praca z materiałem do samokształcenia (np. Jupyter Notebook)	5
	Praca z laboratorium cyfrowym (np. CodeRunner)	
	Inne (jakie?)	
SUMA GODZIN		40
LICZBA PUNKTÓW ECTS DLA PRZEDMIOTU		1.5

* proszę wskazać z proponowanych przykładów pracy własnej studenta właściwe dla opisywanego modułu lub/i zaproponować inne

4. Kryteria oceniania wg skali stosowanej w UAM

Ocena	Kryterium
bardzo dobry (bdb; 5,0)	od 83% punktów
dobry plus (+db; 4,5)	od 75% punktów
dobry (db; 4,0)	od 67% punktów
dostateczny plus (+dst; 3,5)	od 59% punktów
dostateczny (dst; 3,0)	od 50% punktów
niedostateczny (ndst; 2,0)	poniżej 50% punktów