SYLABUS PRZEDMIOTU

Cybernetyczne działania wojenne

I. Informacje ogólne

Nazwa przedmiotu	Cybernetyczne działania wojenne
Kod przedmiotu	CDW
Rodzaj przedmiotu	specjalistyczny
Kierunek studiów	Informatyka
Poziom kształcenia	II stopień
Profil kształcenia	Ogólnoakademicki
Rok studiów	II
Rodzaje zajęć i liczba godzin	
Wykład	15
Ćwiczenia	0
Laboratoria	0
Praktyki	0
Liczba punktów ECTS	1.5

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

- dr Jacek Raubo jraubo@amu.edu.pl / jacek.raubo@protonmail.com

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

II. Informacje szczegółowe

1. Cele przedmiotu

Przedmiot stawia następujące cele:

- wskazanie na wzrost znaczenia cyberbezpieczeństwa w sferze aktywności współczesnych sił zbrojnych oraz służb specjalnych na całym świecie, z

podkreśleniem nowych możliwości działania w toku konfliktów zbrojnych, ale również w okresie pokoju;

- zauważenie militaryzacji i sekurytyzacji domeny cyber, odnoszące się do budowania potencjału defensywnego oraz ofensywnego we współczesnych siłach zbrojnych oraz po stronie służb specjalnych;

- uzyskanie mapy wzywań odnoszących się do możliwości wystąpienia wrogiej aktywności względem domeny cyber w Polsce, bazując na możliwości pojawienia się negatywnych działań po stronie państw oraz podmiotów niepaństwowych, działających samodzielnie lub z inspiracji państw;

- nabycie perspektywy pozwalającej odpowiednio definiować własny wkład w cyberbezpieczeństwo, jako element składowy rozwoju koncepcji odporności państwa w XXI w., bazując na idei obrony powszechnej/obrony totalnej;

- próba budowy świadomości kontrwywiadowczej w zakresie możliwości spotkania się z wrogą aktywnością w domenie cyber, będącą pochodną cyberszpiegostwa lub cyberuderzeń wynikłych z pobudek politycznych, wojskowych, szpiegowskich, a także gospodarczych.

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

Posiadanie podstawowej wiedzy w obrębie zrozumienia cyberbezpieczeństwa, jako elementu kształtującego szerszy obraz bezpieczeństwa.

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:
CDW_01	KINF2_W02 KINF2_U11 KINF2_K06	Potrafi zrozumieć znaczenie cyberbezpieczeństwa dla całościowego problemu procesu zapewnienia odpowiedniego poziomu bezpieczeństwa państwa w XXI w.
CDW_02	KINF2_W02 KINF2_U11 KINF2_K03 KINF2_K06	Potrafi zauważyć możliwość wykorzystania przez obce państwa lub struktury niepaństwowe domeny cyber do działań szpiegowskich oraz wojskowych wymierzonych w jego państwo.
CDW_03	KINF2_W02 KINF2_U11 KINF2_K03 KINF2_K06	Potrafi zrozumieć możliwość wykorzystania przez obce państwa lub struktury niepaństwowe domeny cyber do działań szpiegowskich względem własnych zasobów informacji, a także zasobów znajdujących się po stronie instytucji/firmy, w której pracuje.
CDW_04	KINF2_W02 KINF2_U11 KINF2_K06	Potrafi zauważyć rolę i znaczenie domeny cyber dla całościowego systemu obronnego państwa w warunkach nowych sposobów prowadzenia działań zbrojnych i uderzeń niekinetycznych w toku operacji hybrydowych.
CDW_05	KINF2_W06 KINF2_U11 KINF2_K02 KINF2_K06	Potrafi zrozumieć zróżnicowane postawy względem cyberbezpieczeństwa definiowane przez system polityczny danego państwa oraz formy zabezpieczenia jego interesów narodowych.
CDW_06	KINF2_W06 KINF2_U07 KINF2_U09 KINF2_K02	Rozumie potrzebę przekładania własnych działań zawodowych i pozazawodowych na stworzenie odpowiedniego poziomu cyberbezpieczeństwa oraz odporności systemu obronnego państwa.

	KINF2_K04	
CDW_07	KINF2_W06 KINF2_U07 KINF2_U09 KINF2_U11 KINF2_K02 KINF2_K04	Rozumie wymóg poznawania innych niż techniczne aspektów cyberbezpieczeństwa.
CDW_08	KINF2_W06 KINF2_U07 KINF2_U09 KINF2_K04	Rozumie potrzebę współpracy z osobami zajmującymi się cyberbezpieczeństwem z różnych perspektyw naukowych oraz zawodowych.

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		15	00	16	
1.	CDW_1, CDW_2, CDW_3, CDW_06, CDW_08	2		2	Nowa domena działań, czyli jak państwa oraz sojusze obronne postrzegają cyberprzestrzeń w ujęciu wywiadów oraz wojska
2.	CDW_02, CDW_03, CDW_06, CDW_07, CDW_08	2		2	Kryptologia i rozwój SIGINT-u jako kluczowego źródła pozyskiwania danych wywiadowczych w XX i XXI w., czyli o tym, czy cyberszpiegostwo staje się niezbędne
3.	CDW_01, CDW_02, CDW_04, CDW_05, CDW_07	2		2	Cyberprzestrzeń pełnoprawną domeną prowadzenia działań zbrojnych, czyli jak współczesne konflikty zbrojne przechodzą do cyberprzestrzeni – od Iraku 1991 do Górskiego Karabachu 2020
4.	CDW_01, CDW_02, CDW_04, CDW_05, CDW_07	2		2	C4ISTR, czyli gdzie cyberbezpieczeństwo zaczyna decydować o współczesnych sukcesach oraz porażkach sił zbrojnych
5.	CDW_05, CDW_07	3		4	Chińsko-amerykańska „wojna" o cyberprzestrzeń, czyli jak kształt rywalizacji mocarstw globalnych jest definiowany względami cyberbezpieczeństwa
6.	CDW_05, CDW_07	2		2	Państwo Izrael, czyli przykład państwa, w którym wojsko i służby specjalne rozumieją strategiczne potrzeby oraz możliwości wykorzystania domeny cyber na Bliskim Wschodzie

7.	CDW_05, CDW_07	2		2	Cyberprzestrzeń i WRE czyli jak zrodził się rosyjski pomysł na ograniczenie dysproporcji względem państw NATO

5. Zalecana literatura

1) Bezpieczeństwo funkcjonowania w cyberprzestrzeni, Sylwia Wojciechowska-Filipek, Zbigniew Ciekanowski, CeDeWu.pl, 2016.
2) Chiny 5.0. Jak powstaje cyfrowa dyktatura, Kai Strittmatter , Wydawnictwo W.A.B., 2020.
3) Cyberbezpieczeństwo, red. Cezary Banasiński i Marcin Rojszczak, Wolters Kluwer, 2020.
4) Cyberbezpieczeństwo jako podstawa bezpiecznego państwa i społeczeństwa w XXI wieku, Marek Górka, Difin, 2014.
5) Cyberbezpieczeństwo. Podejście systemowe, Jerzy Krawiec, Oficyna Wydawnicza Politechniki Warszawskiej, 2019.
6) Cyberprzestrzeń jako nowy wymiar rywalizacji i współpracy państw, Miron Lakomy, Wydawnictwo Uniwersytetu Śląskiego, 2015.
7) Cyberwojna. Metody działania hakerów, Dawid Farbaniec, Wydawnictwo Helion, 2018.
8) Inteligencja sztuczna, rewolucja prawdziwa. Chiny, USA i przyszłość świata, Lee Kai-Fu, Media Rodzina 2019.
9) Nowy rodzaj wojny. Media społecznościowe jako broń, P.W. Singer, Emerson T. Brooking, vis-a-vis Etiuda
10) Stany Zjednoczone a międzynarodowe bezpieczeństwo cybernetyczne, Dziwisz Dominika, Self Publishing, 2015.

V. 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 modułu zajęć/przedmiotu									
	CDW: 01, 02, 03, 04, 05, 06, 07									
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										
…										

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	5
	Czytanie wskazanej literatury	20
	Przygotowanie pracy pisemnej, raportu, prezentacji, itp.	0
	Przygotowanie projektu	0
	Przygotowanie pracy semestralnej	0
	Przygotowanie do egzaminu/zaliczenia	0
	Praca z materiałem do samokształcenia (np. Jupyter Notebook)	0
	Praca z laboratorium cyfrowym (np. Code Runner)	0
	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