Polityka cyberbezpieczeństwa. Cybernetyczne działania wojenne

Sylabus zajęć

Informacje podstawowe

Kierunek studiów Informatyka - przedmioty do wyboru **Specjalność** - **Jednostka organizacyjna** Wydział Matematyki i Informatyki **Poziom studiów** studia drugiego stopnia poinżynierskie **Forma studiów** studia stacjonarne **Profil studiów** profil ogólnoakademicki	**Cykl dydaktyczny** 2023/24 **Kod zajęć** 06INFPWS.4200000HS.01052.23 **Języki wykładowe** polski **Obligatoryjność** Fakultatywny **Blok zajęciowy** Przedmioty humanistyczne i społeczne

Koordynator zajęć	Sebastian Wojciechowski, Jacek Raubo
Prowadzący zajęcia	Sebastian Wojciechowski, Jacek Raubo

Okres	**Forma zajęć / liczba godzin / forma zaliczenia**	**Liczba punktów ECTS**
Semestr letni	• Wykład: 15, Zaliczenie z oceną • Ćwiczenia: 15, Zaliczenie z oceną	3

Cele kształcenia dla zajęć

Kod	Cel
C1	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.
C2	Zauważenie militaryzacji i sekurytyzacji domeny cyber, odnoszące się do budowania potencjału defensywnego oraz ofensywnego we współczesnych siłach zbrojnych oraz po stronie służb specjalnych.
C3	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.
C4	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.
C5	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.
C6	Poznanie źródeł, tendencji oraz znaczenia rewolucji informatycznej.
C7	Nabycie umiejętności identyfikowania i charakteryzowania kluczowych wyzwań oraz zagrożeń dotyczących cyberbezpieczeństwa.
C8	Zdobycie wiedzy dotyczącej "miękkich" oraz "twardych" zagrożeń z zakresu cyberbezpieczeństwa.
C9	Zdobycie wiedzy z zakresu zwalczania i prognozowania cyberzagrożeń.

Wymagania wstępne

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

Efekty uczenia się dla zajęć

Kod	Efekty uczenia się dla zajęć w zakresie	Efekty uczenia się dla kierunku	Metody weryfikacji osiągnięcia efektów uczenia się dla zajęć
Wiedzy – Student/ka:			
W1	rozumie znaczenie cyberbezpieczeństwa dla całościowego problemu procesu zapewnienia odpowiedniego poziomu bezpieczeństwa państwa w XXI w.	INF_K4_W02	Kolokwium pisemne
W2	rozumie 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.	INF_K4_W02	Kolokwium pisemne
W3	rozumie zróżnicowane postawy względem cyberbezpieczeństwa definiowane przez system polityczny danego państwa oraz formy zabezpieczenia jego interesów narodowych.	INF_K4_W06	Kolokwium pisemne

Kod	Efekty uczenia się dla zajęć w zakresie	Efekty uczenia się dla kierunku	Metody weryfikacji osiągnięcia efektów uczenia się dla zajęć
W4	rozumie potrzebę przekładania własnych działań zawodowych i pozazawodowych na stworzenie odpowiedniego poziomu cyberbezpieczeństwa oraz odporności systemu obronnego państwa.	INF_K4_W04	Kolokwium pisemne
W5	rozumie wymóg poznawania innych niż techniczne aspektów cyberbezpieczeństwa.	INF_K4_W06	Kolokwium pisemne
W6	rozumie potrzebę współpracy z osobami zajmującymi się cyberbezpieczeństwem z różnych perspektyw naukowych oraz zawodowych.	INF_K4_W06	Kolokwium pisemne
W7	zna podstawowe pojęcia oraz zjawiska z zakresu bezpieczeństwa i cyberbezpieczeństwa oraz potrafi wskazać cechy cyberprzestrzeni.	INF_K4_W03	Zadania cząstkowe wykonywane podczas zajęć
W8	zna "miękkie" wyzwania i zagrożenia dla polityki cyberbezpieczeństwa.	INF_K4_W06	Zadania cząstkowe wykonywane podczas zajęć
W9	rozumie istotę "twardych" wyzwań i zagrożeń dla polityki bezpieczeństwa oraz potrafi scharakteryzować ich przykłady, w tym wskazać znaczenie czy następstwa.	INF_K4_W06	Zadania cząstkowe wykonywane podczas zajęć
Umiejętności – Student/ka:			
U1	zna formy i metody zwalczania cyberzagrożeń; potrafi ocenić ich skuteczność wskazując mocne i słabe strony; umie prognozować nowe potencjalne zagrożenia.	INF_K4_U07, INF_K4_U11	Esej
Kompetencji społecznych – Student/ka:			
K1	zauważa możliwość wykorzystania przez obce państwa lub struktury niepaństwowe domeny cyber do działań szpiegowskich oraz wojskowych wymierzonych w jego państwo.	INF_K4_K03, INF_K4_K06	Kolokwium pisemne
K2	zauważa rolę i znaczenie domeny cyber dla całościowego systemu obronnego państwa w warunkach nowych sposobów prowadzenia działań zbrojnych i uderzeń niekinetycznych w toku operacji hybrydowych.	INF_K4_K06	Kolokwium pisemne
K3	potrafi wskazać przyczyny, przejawy oraz następstwa rewolucji informatycznej; rozumie ich kontekst społeczny oraz technologiczny, a także powiązania ze sferą bezpieczeństwa.	INF_K4_K02	Zadania cząstkowe wykonywane podczas zajęć
K4	potrafi wytłumaczyć formy i przykłady ich stosowania.	INF_K4_K01	Zadania cząstkowe wykonywane podczas zajęć

Treści programowe dla zajęć

Lp.	Treści programowe dla zajęć	Efekty uczenia się dla zajęć	Formy zajęć

Lp.	Treści programowe dla zajęć	Efekty uczenia się dla zajęć	Formy zajęć
1.	Nowa domena działań, czyli jak państwa oraz sojusze obronne postrzegają cyberprzestrzeń w ujęciu wywiadów oraz wojska.	W1, W2, W4, W6, K1	Wykład
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.	W2, W4, W5, W6, K1	Wykład
3.	Cyberprzestrzeń pełnoprawną domeną prowadzenia działań zbrojnych, czyli jak współczesne konflikty zbrojne przechodzą do cyberprzestrzeni – od Iraku 1991 do Górskiego Karabachu 2020.	W1, W3, W5, K1, K2	Wykład
4.	C4ISTR, czyli gdzie cyberbezpieczeństwo zaczyna decydować o współczesnych sukcesach oraz porażkach sił zbrojnych.	W1, W3, W5, K1, K2	Wykład
5.	Chińsko-amerykańska „wojna” o cyberprzestrzeń, czyli jak kształt rywalizacji mocarstw globalnych jest definiowany względami cyberbezpieczeństwa.	W3, W5	Wykład
6.	Państwo Izrael, czyli przykład państwa, w którym wojsko i służby specjalne rozumieją strategiczne potrzeby oraz możliwości wykorzystania domeny cyber na Bliskim Wschodzie.	W3, W5	Wykład
7.	Cyberprzestrzeń i WRE czyli jak zrodził się rosyjski pomysł na ograniczenie dysproporcji względem państw NATO.	W3, W5	Wykład
8.	Wprowadzenie do polityki bezpieczeństwa i cyberbezpieczeństwa.	W7	Ćwiczenia
9.	Rewolucja informatyczna i główne jej tendencje.	K3	Ćwiczenia
10.	"Miękkie" zagrożenia i wyzwania dla polityki cyberbezpieczeństwa (np. cyfrowa przepaść, cyberszpiegostwo, hacking itp.).	W8, K4	Ćwiczenia
11.	"Twarde" zagrożenia i wyzwania dla polityki cyberbezpieczeństwa (np. cyberwojny, cyberterroryzm itp.).	W9	Ćwiczenia
12.	Zwalczanie cyberzagrożeń oraz prognoza ich przyszłej ewolucji.	U1	Ćwiczenia

Informacje dodatkowe

Forma zajęć	Metody i formy prowadzenia zajęć
Wykład	Wykład z prezentacją multimedialną wybranych zagadnień, Wykład konwersatoryjny, Wykład problemowy, Dyskusja
Ćwiczenia	Wykład z prezentacją multimedialną wybranych zagadnień, Dyskusja, Metoda analizy przypadków

Forma zajęć	Warunki zaliczenia zajęć
Wykład	Warunkiem przystąpienia do kolokwium pisemnego jest uzyskanie zaliczenia z laboratoriów. Na końcową ocenę składa się wynik uzyskany na kolokwium. Skala ocen: 1. bardzo dobry (bdb; 5,0) – od 83% punktów, 2. dobry plus (db plus; 4,5) – od 75% punktów, 3. dobry (db; 4,0) – od 67% punktów, 4. dostateczny plus (dst plus; 3,5) – od 59% punktów, 5. dostateczny (dst; 3,0) – od 50% punktów, 6. niedostateczny (ndst; 2,0) – poniżej 50% punktów.
Ćwiczenia	Końcowa ocena składa się z następujących elementów: 1. esej – 60%, 2. zadania wykonywane podczas zajęć – 40%. Skala ocen: 1. bardzo dobry (bdb; 5,0) – od 83% punktów, 2. dobry plus (db plus; 4,5) – od 75% punktów, 3. dobry (db; 4,0) – od 67% punktów, 4. dostateczny plus (dst plus; 3,5) – od 59% punktów, 5. dostateczny (dst; 3,0) – od 50% punktów, 6. niedostateczny (ndst; 2,0) – poniżej 50% punktów.

Literatura

Obowiązkowa

1. Bezpieczeństwo funkcjonowania w cyberprzestrzeni, Sylwia WojciechowskaFilipek, 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. M. Lakomy, Cyberprzestrzeń jako nowy wymiar rywalizacji i współpracy państw, Katowice 2018.
6. A. Podraza, P. Potakowski, K. Wiak (red.), Cyberterroryzm zagrożeniem XXI wieku. Perspektywa politologiczna i prawna, Warszawa 2015. M. Siwicki, Cyberprzestępczość, Warszawa 2017.

Dodatkowa

1. Cyberbezpieczeństwo. Podejście systemowe, Jerzy Krawiec, Oficyna Wydawnicza Politechniki Warszawskiej, 2019.
2. Cyberprzestrzeń jako nowy wymiar rywalizacji i współpracy państw, Miron Lakomy, Wydawnictwo Uniwersytetu Śląskiego, 2015.
3. Cyberwojna. Metody działania hakerów, Dawid Farbaniec, Wydawnictwo Helion, 2018.
4. Inteligencja sztuczna, rewolucja prawdziwa. Chiny, USA i przyszłość świata, Lee Kai-Fu, Media Rodzina 2019.
5. Nowy rodzaj wojny. Media społecznościowe jako broń, P.W. Singer, Emerson T. Brooking, vis-a-vis Etiuda
6. Stany Zjednoczone a międzynarodowe bezpieczeństwo cybernetyczne, Dziwisz Dominika, Self Publishing, 2015.
7. P. Williams, M. McDonald (eds.), Security Studies, An Introduction, London – New York 2018.
8. CyberPolicy Review Biuletyn PIB NASK, ISSN 2657-8360. M. Castells, Społeczeństwo sieci, Warszawa 2015.

Nakład pracy studenta i punkty ECTS

Rodzaje zajęć studenta	Średnia liczba godzin* przeznaczonych na zrealizowane rodzaje zajęć
Wykład	15
Ćwiczenia	15
Przygotowanie do zajęć	5

Czytanie wskazanej literatury	15
Przygotowanie pracy pisemnej	10
Przygotowanie do zaliczenia	10
Inne	5
Łączny nakład pracy studenta	**Liczba godzin** 75
Liczba punktów ECTS	**ECTS** 3

* godzina (lekcyjna) oznacza 45 minut

Efekty uczenia się dla kierunku

Kod	Treść
INF_K4_K01	Absolwent/ka jest gotów/gotowa do precyzyjnego formułowania pytań służących pogłębieniu własnego zrozumienia danego tematu lub odnalezienia brakujących elementów rozumowania
INF_K4_K02	Absolwent/ka jest gotów/gotowa do zasięgania opinii ekspertów przy rozwiązywaniu problemów teoretycznych i praktycznych
INF_K4_K03	Absolwent/ka jest gotów/gotowa do zrozumienia i docenienia znaczenia uczciwości intelektualnej w działaniach własnych i innych osób; postępuje etycznie
INF_K4_K06	Absolwent/ka jest gotów/gotowa do pogłębiania świadomości roli informatyki w kształtowaniu życia społecznego
INF_K4_U07	Absolwent/ka potrafi wyrażać krytyczne opinie na temat architektury oraz użyteczności wykorzystywanych systemów informatycznych
INF_K4_U11	Absolwent/ka potrafi pozyskiwać informacje z literatury, baz wiedzy, Internetu oraz innych wiarygodnych źródeł, integrować je, dokonywać ich interpretacji oraz wyciągać wnioski i formułować opinie
INF_K4_W02	Absolwent/ka zna i rozumie współczesny stan badań i tendencje rozwojowe w wiodących obszarach informatyki
INF_K4_W03	Absolwent/ka zna i rozumie w pogłębionym stopniu współczesne metody, narzędzia i technologie informatyczne właściwe dla wybranych obszarów zastosowań niezbędne przy budowie złożonych systemów informatycznych oraz przy prowadzeniu prac badawczo-rozwojowych
INF_K4_W04	Absolwent/ka zna i rozumie zasady rozwiązywania problemów z wykorzystaniem zaawansowanych algorytmów i metod informatycznych
INF_K4_W06	Absolwent/ka zna i rozumie zagadnienia prawne i społeczne aspekty informatyki, w tym odpowiedzialności zawodowej i etycznej, kodeksów etycznych, własności intelektualnej, prywatności i swobód obywatelskich, ryzyka i odpowiedzialności związanej z systemami informatycznymi