**KARTA PRZEDMIOTU**

Cykl kształcenia od roku akademickiego: 2024/2025

1. **Dane podstawowe**

|  |  |
| --- | --- |
| Nazwa przedmiotu | Analiza konfliktów z cyberbezpieczeństwa |
| Nazwa przedmiotu w języku angielskim | Analysis of Conflicts in Cybersecurity |
| Kierunek studiów  | Bezpieczeństwo narodowe |
| Poziom studiów (I, II, jednolite magisterskie) | II stopień |
| Forma studiów (stacjonarne, niestacjonarne) | Stacjonarne |
| Dyscyplina | Nauki o polityce i administracji, Nauki oBezpieczeństwie |
| Język wykładowy | Polski |

|  |  |
| --- | --- |
| Koordynator przedmiotu | Urszula Soler |

|  |  |  |  |
| --- | --- | --- | --- |
| Forma zajęć *(katalog zamknięty ze słownika)* | Liczba godzin | semestr | Punkty ECTS |
| wykład |  |  | 4 |
| konwersatorium |  |  |
| ćwiczenia | 30 | I |
| laboratorium |  |  |
| warsztaty |  |  |
| seminarium |  |  |
| proseminarium |  |  |
| lektorat |  |  |
| praktyki |  |  |
| zajęcia terenowe |  |  |
| pracownia dyplomowa |  |  |
| translatorium |  |  |
| wizyta studyjna |  |  |

|  |  |
| --- | --- |
| Wymagania wstępne | Znajomość podstawowych pojęć z zakresu cyberbezpieczeństwa |

1. **Cele kształcenia dla przedmiotu**

|  |
| --- |
| C1 - Zapoznanie z głównymi zagadnieniami dotyczącymi cyberbezpieczeostwa |
| C2 - Przekazanie wiedzy nt. sposobów przebiegów konfliktów z cyberprzestrzeni i analizy ich rozwoju |
| C3 - Ukierunkowanie na potrzebę samodzielnego, krytycznego analizowania zjawisk w obszarze |

1. **Efekty uczenia się dla przedmiotu wraz z odniesieniem do efektów kierunkowych**

|  |  |  |
| --- | --- | --- |
| Symbol | Opis efektu przedmiotowego | Odniesienie do efektu kierunkowego |
| WIEDZA |
| W\_01 | Zna złożony charakter uwarunkowań bezpieczeństwa globalnego, systemów bezpieczeństwa państwa, a także bezpieczeństwa międzynarodowego, w tym instytucji międzynarodowych | K\_W05 |
| W\_02 | Zna i definiuje zjawiska w obszarze cyberbezpieczeństwa | K\_W03 |
| UMIEJĘTNOŚCI |
| U\_01 | Potrafi wykorzystywać pogłębioną wiedzę teoretyczną w rozwiązywaniu problemów związanych z cyberbezpieczeństwem państwa i w wymiarze międzynarodowym | K\_U03 |
| U\_02 | Potrafi prawidłowo ocenia zagrożenia w cyberprzestrzeni, a także identyfikowa ich przyczyny | K\_U05 |
| KOMPETENCJE SPOŁECZNE |
| K\_01 | Jest gotów do angażowania się w działania wspierająceprocesy bezpieczeństwa międzynarodowego w cyberprzestrzeni | K\_K01, K\_K02 |

1. **Opis przedmiotu/ treści programowe**

|  |
| --- |
| 1. Bezpieczeństwo w cyberprzestrzeni – historia cyberprzestrzeni i prognozy przyszłości cyberprzestrzeni, definicja zagrożeń cybernetycznych, problem rozróżnienia ataków cybernetycznych2. Bezpieczeństwo w erze Big Data – konsekwencje analizy wielkich zbiorów danych, możliwe naruszenia prawa do prywatności, prawo do bycia zapomnianym, bezpieczeństwo danych osobowych, RODO/GDPR w praktyce3. Wojna w cyberprzestrzeni – problem atrybucji ataku cybernetycznego, prawne aspekty wojny w cyberprzestrzeni, kontrowersje na temat możliwości prowadzenia wojny w cyberprzestrzeni4. Rewolucja IT w kontekście militarnym - przyszłość Internetu, nowy „cybernetyczny” żołnierz, IoT, sztuczna inteligencja, Big Data, AR na użytek wojska5. Cyberprzestrzeń jako wymiar rywalizacji państw (Chiny, USA, UE, NATO…) wywiad cybernetyczny, rywalizacja gospodarcza/wywiad gospodarczy, Internet jako narzędzie propagandy |

1. **Metody realizacji i weryfikacji efektów uczenia się**

|  |  |  |  |
| --- | --- | --- | --- |
| Symbol efektu | Metody dydaktyczne*(lista wyboru)* | Metody weryfikacji*(lista wyboru)* | Sposoby dokumentacji*(lista wyboru)* |
| WIEDZA |
| W\_01 | Ćwiczenia | zaliczenie | protokół |
| UMIEJĘTNOŚCI |
| U\_01 | ćwiczenia Analiza aktualnych konfliktów w cyberprzestrzeni i tekstów źródłowych w Internecie | zaliczenie | protokół |
| U\_02 | ćwiczenia Studium przypadku | zaliczenie | protokół |
| KOMPETENCJE SPOŁECZNE |
| K\_01 | Dyskusja stacjonarna | zaliczenie | protokół |

1. **Kryteria oceny, wagi…**

Systematyczna obecność na zajęciach i aktywność na nich. Udział w wydarzeniach (konferencje, seminaria) związanych z tematyką zajęć. Zaliczenie ćwiczeń.

**Obciążenie pracą studenta**

|  |  |
| --- | --- |
| Forma aktywności studenta | Liczba godzin |
| Liczba godzin kontaktowych z nauczycielem  | **30** |
| Liczba godzin indywidualnej pracy studenta | **15** |

1. **Literatura**

|  |
| --- |
| Literatura podstawowa |
| M. Wrzosek, *Operacje w cyberprzestrzeni. Założenia teoretyczne i praktyka*, Kwartalnik Bellona 2016; 687 (4): 42-59.D. Van Puyvelde , A. F. Brantly, *Cybersecurity: Politics*, Governance and Conflict in Cyberspace 1st Edition, Polity; 1st edition (September 3, 2019). |
| Literatura uzupełniająca |
| K. Chałubińska-Jentkiewicz, *The Role of Cybersecurity in the Public Sphere - The European Dimension*, Lex Localis, Maribor, 2022.M. B. Gazula, *Cyber Warfare Conflict Analysis and Case Studies*, Massachusetts Institute of Technology June 2017.M. Kapiuk, A. Makuch, U. Soler, *The role of the Cybersecurity Strategy of the Republic of Poland in ensuring cybersecurity*, “Polish Political Science Yearbook”, vol. 52(3) (2023), pp. 155–163, DOI: https://doi.org/10.15804/ppsy2023833 |