## *Załącznik 2 do WSZJK (P1)*

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **KARTA PRZEDMIOTU DLA NABORU 2023/2024**  **FORMA STUDIÓW: NIESTACJONARNA** | | | | |
| **INFORMACJE OGÓLNE** | | | | |
| **1.** **Nazwa przedmiotu** Cyberzagrożenia bezpieczeństwa państwa | | | | |
| 1. **2. Nazwa kierunku** Bezpieczeństwo Narodowe | | | | |
| 1. **3. Poziom kształcenia** studia drugiego stopnia | | | | |
| 1. **4. Liczba punktów ECTS** 3 | | | | |
| 1. **5. Liczba godzin w semestrze**  |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | | semestr | w | ćw | lab/lek | prj/zp | pws | prk | | III | 9 | 9 |  |  |  |  | | | | | |
| 1. **6. Język wykładowy** językpolski | | | | |
| 1. **7. Wykładowca** | | | | |
| **INFORMACJE SZCZEGÓŁOWE** | | | | |
| **8. Wymagania wstępne** | | | | |
| brak | | | | |
| **9. Cele przedmiotu** | | | | |
| C1 Przekazanie studentom wiedzy dotyczącej problematyki cyberbezpieczeństwa. | | | | |
| C2 Zapoznanie studentów z polityką cyberbezpieczeństwa Polski i wybranych państw. | | | | |
| **10. Efekty uczenia się w zakresie wiedzy, umiejętności i kompetencji społecznych** | | | | |
| Student, który zaliczył przedmiot: | | | odniesienie do kierunkowych efektów uczenia się | |
| **WIEDZA** | | | | |
| EU01 | Definiuje podstawowe pojęcia z zakresu cyberprzestrzeni oraz ma wiedzę na temat jej specyfiki, uwarunkowań bezpieczeństwa w jej obszarze | | K\_W01, K\_W02 | |
| EU02 | Zna aspekty prawne związane z obszarem cyberbezpieczeństwa. | | K\_W12 | |
| **UMIEJĘTNOŚCI** | | | | |
| EU03 | Analizuje, interpretuje i wyjaśnia bezpieczeństwo w cyberprzestrzeni, jego zagrożenia i działania na rzecz jego zapewnienia | | K\_U01, K\_U04 | |
| **KOMPETENCJE SPOŁECZNE** | | | | |
| EU04 | | Jest gotów w sposób ciągły pogłębiać wiedzę. | K\_K01 | |
| **11. Treści programowe** | | | | |
| **Forma zajęć** – wykłady   1. Wprowadzenie do podstawowych pojęć związanych z cyberbezpieczeństwem. 2. Cyberprzestrzeń i jej ewolucja. 3. Uwarunkowania bezpieczeństwa w obszarze cyberprzestrzeni. 4. Prawne aspekty bezpieczeństwa w cyberprzestrzeni. 5. Zagrożenia w cyberprzestrzeni. 6. Strategia cyberbezpieczeństwa RP. 7. Rola i zadania kluczowych podmiotów publicznych zaangażowanych w aspekty krajowego systemu cyberbezpieczeństwa. 8. Działania służb specjalnych w zakresie zwalczania cyberzagrożeń. | | | | |
| **Forma zajęć** – ćwiczenia   1. Problematyka terminologiczna. Pojęcie cyberbezpieczeństwa. 2. Cyberbezpieczeństwo, rodzaje cyberzagrożeń. 3. Cyberprzestępczość. 4. Cyberterroryzm i jego zwalczanie. 5. Strategie bezpieczeństwa cyberprzestrzeni wybranych państw. 6. Strategia bezpieczeństwa cybernetycznego UE. 7. Wyzwania w cyberprzestrzeni. | | | | |
| **12. Narzędzia/metody dydaktyczne** | | | | |
| 1. wykład | | | | |
| 1. dyskusja | | | | |
| 1. referat w postaci prezentacji multimedialnej | | | | |
| **13. Sposoby oceny** (cząstkowe, końcowe ) | | | | |
| 1. referat | | | | |
| 1. kolokwium | | | | |
| 1. zaliczenie | | | | |
| **14. Obciążenie pracą studenta** | | | | |
| Forma aktywności | | | | liczba godzin |
| 1. Zajęcia z bezpośrednim udziałem nauczyciela oraz konsultacje | | | | 30 |
| 1. Nakład pracy studenta – przygotowanie się do kolokwium i zaliczenia | | | | 25 |
| 1. Nakład pracy studenta – przygotowanie referatu w postaci prezentacji multimedialnej | | | | 20 |
| suma | | | | 75 |
| liczba punktów ECTS | | | | 3 |
| **15. Literatura** | | | | |
| Literatura podstawowa: | | | | |
| 1. Strategie cyberbezpieczeństwa | | | | |
| 1. Krawiec J., Cyberbezpieczeństwo: podejście systemowe, Oficyna Wydawnicza Politechniki Warszawskiej, Warszawa 2019. | | | | |
| 1. Wojciechowska-Filipek S., Ciekanowski Z., Bezpieczeństwo funkcjonowania w cyberprzestrzeni: jednostki, organizacji, państwa, Warszawa 2015. | | | | |
| 1. Górka M., Cyberbezpieczeństwo jako podstawa bezpiecznego państwa i społeczeństwa XXI wieku, Difin, Warszawa 2014. | | | | |
| Literatura uzupełniająca: | | | | |
| 1. Liedel K., Piasecka P., Aleksandrowicz T. R., Bezpieczeństwo w XX wieku: asymetryczny świat, Difin, Warszawa 2011. | | | | |
| 1. Sawicki M., Cyberprzestępczość, C.H. Beck, Warszawa 2013. | | | | |
| 1. Drmola J., Perspectives on cybersecurity, ebook, 2015. | | | | |
| **16. Formy oceny – szczegóły** | | | | |
| Ocena z wykładów – zaliczenie w postaci testu jednokrotnego wyboru (zaliczenie – minimum 51% punktów).  Ocena z ćwiczeń – ocena wynikająca z sumy punktów z referatu i kolokwium (minimum 51% punktów). | | | | |
| **17. Inne przydatne informacje o przedmiocie** | | | | |
| 1. Informacja, gdzie można zapoznać się z materiałami do zajęć, itp. – na stronie Uczelni | | | | |
| 1. Informacje na temat miejsca odbywania zajęć – w salach Uczelni | | | | |
| 1. Informacja na temat terminu zajęć (dzień tygodnia/godzina) – zgodnie z planem zajęć umieszczonym na stronie Uczelni | | | | |
| 1. Informacja na temat konsultacji (godziny + miejsce) – zgodnie z harmonogramem konsultacji umieszczonym na stronie Uczelni | | | | |