**KARTA PRZEDMIOTU**

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Kierunek:**  **BEZPIECZEŃSTWO WEWNĘTRZNE** | | | | |  | | | | |
| **Nazwa przedmiotu: BEZPIECZEŃSTWO CYBERNETYCZNE** | | | | | **Kod przedmiotu:**  **BCyber** | | | | |
| **Rodzaj przedmiotu:**  **Poszerzonych kompetencji B** | | | | | **Rok studiów:**  **II** | **Semestr:**  **IV** | | **Tryb:**  **STACJONARNY** | |
| **Liczba godzin:**  **45** | | | | | **Liczba punktów ECTS:**  **4** | | | **Poziom studiów:**  **I stopień** | |
| **Tytuł, imię i nazwisko; adres e-mailowy wykładowcy/wykładowców:**  prof. dr hab. Piotr Dela, p.dela@uniwersytetkaliski.edu.pl | | | | | | | | | |
| **Informacje szczegółowe:** | | | |  | | | | | |
| **Cele przedmiotu** | | | | | | | | | |
| **C1** przyswoić wiedzą na temat zagrożeń w obszarze cyberprzestrzeni, uwarunkowań prawnych cyberbezpieczeństwa oraz sposobów przeciwdziałania zagrożeniom w cyberprzestrzeni | | | | | | | | | |
| **C2** opanować umiejętność identyfikowania zagrożeń bezpieczeństwa cyberprzestrzeni oraz budowania systemów ochronnychw oparciu o istniejące uwarunkowania prawne i systemowe | | | | | | | | | |
| **C3** gotowość do analizy systemu bezpieczeństwa cyberprzestrzeni, identyfikacji wyzwań w obszarze cyberbezpieczeństwa, pożądanych kierunków przeciwdziałania zagrożeniom oraz prezentację wyników i udział w dyskusji | | | | | | | | | |
| **Wymagania wstępne w zakresie wiedzy, umiejętności,**  **kompetencji społecznych:** | | | | |  | | | | |
| **Efekty kształcenia w zakresie wiedzy, umiejętności oraz kompetencji społecznych** | | | | | | | | | |
| **Efekty uczenia się:** | **Po realizowaniu przedmiotu**  **i potwierdzeniu osiągnięcia efektów kształcenia student:** | | | | | | | **Odniesienie**  **do celów**  **przedmiotu:** | **Odniesienie**  **do efektów uczenia się**  **dla programu:** |
| **EU1** | Ma uporządkowaną wiedzę na temat zagrożeń w obszarze cyberprzestrzeni, uwarunkowań prawnych cyberbezpieczeństwa oraz sposobów przeciwdziałania zagrożeniom w cyberprzestrzeni. | | | | | | | **C1** | **K\_W03**  **K\_W06**  **K\_W11**  **K\_W12**  **K\_W13** |
| **EU2** | Potrafi identyfikować zagrożeń bezpieczeństwa cyberprzestrzeni oraz zasady budowania systemów ochronnychw oparciu o istniejące uwarunkowania prawne i systemowe. | | | | | | | **C2** | **K\_U01**  **K\_U05**  **K\_U06**  **K\_U07**  **K\_U10** |
| **EU3** | Jest gotów do dokonania analizy systemu bezpieczeństwa cyberprzestrzeni, identyfikacji wyzwań w obszarze cyberbezpieczeństwa, pożądanych kierunków przeciwdziałania zagrożeniom oraz prezentację uzyskanych wyników i udział w dyskusji. | | | | | | | **C3** | **K\_K02**  **K\_K03**  **K\_K05** |
| **Treści programowe** | | | |  | | | | | |
| **Treści**  **Programowe:** |  | | | **Forma zajęć:** | | | | **Liczba**  **godzin** | **Odniesienie**  **do efektów uczenia się** |
|  |  | | | **Konwersatoria:** | | | | **15** |  |
| **TP1** | Istota cyberprzestrzeni i jej znaczenie we współczesnym świecie | | | | | | | **3** | **EU1** |
| **TP2** | Ewolucja zagrożeń w cyberprzestrzeni | | | | | | | **2** | **EU1** |
| **TP3** | Ataki na poufność informacji | | | | | | | **2** | **EU1** |
| **TP4** | Ataki na integralność informacji | | | | | | | **2** | **EU1** |
| **TP5** | Ataki na dostępność informacji | | | | | | | **2** | **EU1** |
| **TP6** | Dezinformacja i propaganda | | | | | | | **2** | **EU1** |
| **TP7** | Znaczenie bezpieczeństwa cyberprzestrzeni dla rozwoju państwa | | | | | | | **2** | **EU1, EU2** |
|  |  | | | **Laboratoria:** | | | | **30** |  |
| **TP1** | Ewolucja zagrożeń w cyberprzestrzeni | | | | | | | **4** | **EU2** |
| **TP2** | Studium przypadku – ataki na poufność informacji | | | | | | | **4** | **EU2** |
| **TP3** | Studium przypadku – ataki na integralność informacji | | | | | | | **4** | **EU2** |
| **TP4** | Studium przypadku – ataki na dostępność informacji | | | | | | | **4** | **EU2** |
| **TP5** | Informacja jako narzędzie ataku – manipulacje informacją. | | | | | | | **4** | **EU2** |
| **TP6** | Metody i sposoby eliminowania zagrożeń w cyberprzestrzeni | | | | | | | **4** | **EU2, EU3** |
| **TP7** | Strategie i doktryny bezpieczeństwa | | | | | | | **4** | **EU2, EU3** |
| **TP8** | Prognozowanie zagrożeń bezpieczeństwa cyberprzestrzeni | | | | | | | **2** | **EU2, EU3** |
| **Narzędzia dydaktyczne:** | | | | | | | | | |
| **1.** Konwersatoria - sala z systemem multimedialnym.  **2.** Laboratoria – sala komputerowa z dostępem do sieci Internet**.** | | | | | | | | | |
| **Metody weryfikacji osiągnięcia efektów kształcenia** | | | | | | | | | |
| **Efekt**  **uczenia się:** | | **Forma weryfikacji i walidacji efektów kształcenia** | | | | | | | |
| **Wiedza faktograficzna** | | | **Wiedza praktyczna**  **umiejętności praktyczne** | | **Umiejętności kognitywne** | **Kompetencje społeczne**  **postawy** | |
| **EU1** | | **X** | | |  | |  |  | |
| **EU2** | |  | | | **X** | | **X** |  | |
| **EU3** | |  | | |  | |  | **X** | |
| **Kryteria oceny osiągnięcia efektów kształcenia** | | | | | | | | | |
| **F – formujące:** | | | |  | | | | | |
| **F1.** Oceny ze sprawdzianów pisemnych wiedzy objętej treścią wykładów i ćwiczeń.  **F2.** Ocena z aktywności na ćwiczeniach.  **F3.** Ocena z wystąpień na ćwiczeniach.  **F4.** Ocena za sposób prowadzenia analizy danego zdarzenia w ramach studium przypadków.  **F5.** Ocena efektów pracy w ramach samokształcenia.  **F6.** Ocena umiejętności z zakresu prowadzenia dyskusji podczas ćwiczeń. | | | | | | | | | |
| **P – podsumowujące:** | | | |  | | | | | |
| **P1.** Egzamin pisemny z zakresu materiału wykładowego – 100% oceny końcowej wykładów.  **P2.** Oceny z dwóch pisemnych sprawdzianów – 100% oceny końcowej ćwiczeń.  **P3.** Oceny z zadań realizowanych podczas laboratoriów – 100% oceny końcowej ćwiczeń | | | | | | | | | |
| **Skala ocen** | | | | | | | | | |
| **Ocena:** | **Poziom wiedzy, umiejętności, kompetencji personalnych i społecznych:** | | | | | | | | |
| 5,0 | - znakomita wiedza, umiejętności, kompetencje personalne i społeczne | | | | | | | | |
| 4,5 | - bardzo dobra wiedza, umiejętności, kompetencje personalne i społeczne | | | | | | | | |
| 4,0 | - dobra wiedza, umiejętności, kompetencje personalne i społeczne | | | | | | | | |
| 3,5 | - zadowalająca wiedza, umiejętności, kompetencje personalne i społeczne, ale ze znaczącymi   niedociągnięciami | | | | | | | | |
| 3,0 | - zadowalająca wiedza, umiejętności, kompetencje personalne i społeczne, ale z licznymi   błędami | | | | | | | | |
| 2,0 | - niezadowalająca wiedza, umiejętności, kompetencje personalne i społeczne | | | | | | | | |
| **Forma zakończenia:** | | | **Egzamin** | | | | | | |
| **Obciążenie pracą studenta** | | | | | | | | | |
| **Forma aktywności** | | | | | | | | | |
| 1. Godziny kontaktowe z nauczycielem  akademickim : **45**  2. Przygotowanie się do zajęć: **55**  **SUMA: 100** | | | | | | | | | |
| **Literatura** | | | | | | | | | |
| **Podstawowa:**   1. P. Dela, Założenia działań w cyberprzestrzeni, Wydawnictwo Naukowe PWN, Warszawa 2022. 2. R. Janczewski, Cyberwalka. Militarny wymiar działań, Wydawnictwo Naukowe PWN, Warszawa 2023. 3. K. Liderman, Bezpieczeństwo informacyjne. Nowe wyzwania, Wydawnictwo Naukowe PWN, Warszawa 2017. 4. J. Kosiński, Paradygmaty cyberprzestępczości, Dyfin, Warszawa 2015. 5. Artykuły publikowane na łamach czasopisma naukowego „Cybersecurity & cybercrime”, AMW, Gdynia. | | | | | | | | | |
| **Uzupełniająca:**   1. P. Dela, Elementy propagandy w życiu publicznym, Studia Politologiczne, 2019/54, UW, Warszawa 2015. 2. T. Aleksandrowicz, Podstawy walki informacyjnej*,* Editions Spotkania, Warszawa 2016. 3. Ustawy, polityki, strategie i doktryny związane z cyberbezpieczeńswem państwa. | | | | | | | | | |
| **Inne przydatne informacje o przedmiocie:** | | | | | | | | | |
|  | | | | | | | | | |