Załącznik nr 4 do Zarządzenia Nr RD/Z.0201-……..…………..

# KARTA KURSU

|  |  |
| --- | --- |
| Nazwa | Cyberbezpieczeństwo |
| Nazwa w j. ang. | Cybersecurity |

|  |  |  |
| --- | --- | --- |
| Koordynator | dr Maciej Saskowski | Zespół dydaktyczny |
| dr Maciej Saskowski |
| Punktacja ECTS\* | 1 |

## Opis kursu (cele kształcenia)

|  |
| --- |
| Celem kursu jest zapoznanie studentów z podstawowymi zagadnieniami związanymi z cyberbezpieczeństwem. Podczas kursu omawiane są koncepcje psychologiczne leżące u podstaw inżynierii społecznej i jej aspekty etyczne. Prezentowane są narzędzia ułatwiające korzystanie z technik inżynierii społecznej w atakach socjotechnicznych. Omawiane są etapy złożonego ataku phishingowego a także sztuczki stosowane w celu oszukania użytkowników i obrońców. Ponadto student poznaje liczne techniki proaktywnej ochrony przed atakami socjotechnicznymi, a także techniczne sposoby kontroli poczty elektronicznej i narzędzia do analizy potencjalnie podejrzanych wiadomości. |

## Warunki wstępne

|  |  |
| --- | --- |
| Wiedza | - |
| Umiejętności | - |
| Kursy | - |

## Efekty uczenia się

|  |  |  |
| --- | --- | --- |
| Wiedza | Efekt kształcenia dla kursu | Odniesienie do efektów kierunkowych |
| W01. Student zna znaczenie i relacje pomiędzy podstawowymi pojęciami związanymi z cyberbezpieczeństwem (np. cyberprzestępczość, cyberzagrożenia, bezpieczeństwo informacji). | K2\_W01 |
| W02. Student zna podstawowe regulacje prawne i organizacyjne związane z zachowaniem cyberbezpieczeństwa państwa, organizacji i jednostki. | K2\_W05 |
| W03. Student zna typy cyberzagrożeń i cyberprzestępstw oraz wskazuje możliwości przeciwdziałania im i ich zwalczania. | K2\_W01 |

|  |  |  |
| --- | --- | --- |
| Umiejętności | Efekt kształcenia dla kursu | Odniesienie do efektów kierunkowych |
| U01. Student potrafi wykorzystać wiedzę teoretyczną do analizy i charakterystyki wybranych typów cyberzagrożeń. | K2\_U03 |
| U02. Student potrafi w sposób prawidłowy posługiwać się nomenklaturą pojęciową w tematyce cyberbezpieczeństwa. | K2\_U03 |
| U03. |  |

|  |  |  |
| --- | --- | --- |
| Kompetencje społeczne | Efekt kształcenia dla kursu | Odniesienie do efektów kierunkowych |
| K01. Student samodzielnie rozszerza swoją wiedzę w zakresie cyberbezpieczeństwa. | K2\_K01 |
| K02. Student rozumie znaczenie zachowania cyberbezpieczeństwa we współczesnym świecie. | K2\_K03 |
| K03. |  |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Organizacja | | | | | | | |
| Forma zajęć | Wykład (W) | Ćwiczenia w grupach | | | | | |
| A | K | L | S | P | E |
| Liczba godzin | 10 |  | 0 | 0 |  |  |  |

## Opis metod prowadzenia zajęć

|  |
| --- |
| Wykład z wykorzystaniem prezentacji multimedialnych i filmów.  Część zajęć może zostać poprowadzona w sposób aktywizujący studentów (dyskusja na zadany temat). |

## Formy sprawdzania efektów uczenia się

|  |  |
| --- | --- |
| Efekt kierunkowy | Formy sprawdzania |
| W01 | Udział w dyskusji |
| W02 | Udział w dyskusji |
| W03 | Udział w dyskusji |
| U01 | Udział w dyskusji |
| U02 | Udział w dyskusji |
| U03 |  |
| K01 | Udział w dyskusji |
| K02 | Udział w dyskusji |
| K03 |  |

|  |  |
| --- | --- |
| Sposób zaliczenia | Zaliczenie |

|  |  |
| --- | --- |
| Kryteria oceny | Obecność (80%) i aktywność na zajęciach.  Pozytywny wynik z kolokwium kończącego zajęcia (uzyskanie minimum 60% poprawnych odpowiedzi). |

## Treści merytoryczne (wykaz tematów)

|  |
| --- |
| **Wykład**  Podstawy: cyberprzestrzeń, cyberbezpieczeństwo, cyberzagrożenia, cyberprzestępczość, bezpieczeństwo informacyjne, bezpieczeństwo informacji (2h).  Przegląd zaawansowanych cyberzagrożeń (2h).  Wykrywanie i analiza zaawansowanych cyberzagrożeń (2h).  Ofensywna inżynieria społeczna (2h).  Obrona przed socjotechniką (2h). |

|  |
| --- |
| **Ćwiczenia**  - |

## Wykaz literatury podstawowej

|  |
| --- |
| M. Lakomy, Cyberprzestrzeń jako nowy wymiar rywalizacji i współpracy państw, Wydawnictwo UŚ, 2015.  K. Liderman, Bezpieczeństwo informacyjne. Nowe wyzwania, PWN, 2017.  J. Gray, Socjotechniki w praktyce. Podręcznik etycznego hakera, Helion, 2023.  J. DiMaggio, Sztuka wojny cyfrowej, Helion, 2023.  Y. Diogenes, E. Ozkaya - strategie ataku i obrony. Jak osiągnąć najwyższy możliwy stan zabezpieczeń systemu informatycznego. Wydanie III, Helion, 2023.  C. Bravo, Cyberbezpieczeństwo dla zaawansowanych. Skuteczne zabezpieczenia systemu Windows, Linux, IoT i infrastruktury w chmurze, Helion, 2023.  W. Ciemski, Cybersecurity w pytaniach i odpowiedziach, Helion, 2023.  D. Borges, Sztuka prowadzenia cyberkonfliktu. Atak i obrona w czasie rzeczywistym, Helion, 2023. |

## Wykaz literatury uzupełniającej

|  |
| --- |
| M. Górka, Cyberbezpieczeństwo jako podstawa bezpiecznego państwa i społeczeństwa w XXI wieku, Difin, 2014.  Ł. Olejnik, A. Kurasiński, Filozofia cyberbezpieczeństwa, PWN, 2022. |

## Bilans godzinowy zgodny z CNPS (Całkowity Nakład Pracy Studenta)

|  |  |  |
| --- | --- | --- |
| Liczba godzin w kontakcie z prowadzącymi | Wykład | 10 |
| Konwersatorium (ćwiczenia, laboratorium itd.) | 0 |
| Pozostałe godziny kontaktu studenta z prowadzącym | 0 |
| Liczba godzin pracy studenta bez kontaktu z prowadzącymi | Lektura w ramach przygotowania do zajęć | 5 |
| Przygotowanie krótkiej pracy pisemnej lub referatu po zapoznaniu się z niezbędną literaturą przedmiotu | 0 |
| Przygotowanie projektu lub prezentacji na podany temat (praca w grupie) | 0 |
| Przygotowanie do egzaminu/zaliczenia | 10 |
| Ogółem bilans czasu pracy | | 25 |
| Liczba punktów ECTS w zależności od przyjętego przelicznika | | 1 |