**karta przedmiotu**

1. Podstawowe informacje o przedmiocie

|  |  |
| --- | --- |
| Nazwa przedmiotu | Podstawy cyberbezpieczeństwa |
| Rocznik studiów | 2022/23 |
| Kolegium | Kolegium Informatyki Stosowanej |
| Kierunek studiów | Informatyka |
| Poziom kształcenia | Studia pierwszego stopnia - licencjackie |
| Profil kształcenia | Praktyczny |
| Specjalność | - |
| Osoba odpowiedzialna | dr inż. Janusz Korniak |

1. Wymagania wstępne (wynikające z następstwa przedmiotów)

|  |
| --- |
| Technologie sieciowe (CCNA) |

1. Efekty uczenia się i sposób realizacji zajęć
   1. Cele przedmiotu

|  |  |
| --- | --- |
| C1 | Kształcenie wiedzy i powiązanych umiejętności dotyczących identyfikowania zagrożeń w systemach IT i podejmowania środków zaradczych |

* 1. Przedmiotowe efekty uczenia się, z podziałem na wiedzę, umiejętności i kompetencje społeczne, wraz z odniesieniem do efektów uczenia się dla kierunku

|  |  |  |
| --- | --- | --- |
| Lp. | Opis przedmiotowych efektów uczenia się | Odniesienie do efektów uczenia się dla kierunku |
| Po zaliczeniu przedmiotu student w zakresie **wiedzy** | | |
| P\_W01 | Posiada wiedzę z zakresu podstawowych technik bezpieczeństwa oraz przeciwdziałania zagrożeniom | K\_W04 |
| P\_W02 | Rozumie źródła zagrożeń podczas stosowania technologii IT i ich zależności ekonomiczne, prawne i etyczne | K\_W09 |
| Po zaliczeniu przedmiotu student w zakresie **umiejętności** | | |
| P\_U01 | Potrafi przedstawić w formie prezentacji wyniki realizacji projektu | K\_U04 |
| P\_U02 | Potrafi zidentyfikować zagrożenie, zbadać jego działanie i opracować środki zaradcze | K\_U17 |
| P\_U03 | Posługuje się technikami, narzędziami i oprogramowaniem w celu badania zagrożeń i ich przeciwdziałaniu | K\_U18 |

* 1. Formy zajęć dydaktycznych oraz wymiar godzin i punktów ECTS

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Studia stacjonarne (ST) | | | | | | | |
| W | K | Ćw | L | ZP | P | eL | ECTS |
| 14 | - | - | 14 | - | 24 | - | 6 |

* 1. Metody realizacji zajęć dydaktycznych

|  |  |
| --- | --- |
| Formy zajęć | Metoda realizacji |
| Wykład | Wiedza przekazywana w postaci wykładu przeplatanego formami: podawczej, problemowej i konwersatoryjnej. Ponadto wykładowca zadaje temat do samodzielnych studiów w celu poszerzenia wiedzy. |
| Laboratorium | Zajęcia polegające na wykonywaniu eksperymentów związanych z analizą zagrożeń oraz badaniem wybranych technik zaradczych i ich wdrażaniem. Studenci otrzymują zestaw instrukcji na pierwszych zajęciach obejmujących ćwiczenia podstawowe z instrukcją wyjaśniającą krok po kroku zadania do wykonania oraz ćwiczenia problemowe, w których sprecyzowany jest cel jaki ma być osiągnięty bez podania sposobu. Zajęcia realizowane z wykorzystaniem rzeczywistego sprzętu (typowego dla sieci produkcyjnych) w warunkach zbliżonych do rzeczywistej eksploatacji sieci. |
| Projekt | Zajęcia polegają na wykonaniu projektu, który stanowi analizę wybranych zagrożeń, sposobów zaradczych i technik oraz metod przeciwdziałania. Student przeprowadza prosty test penetracyjny wykrywający dane zagrożenie. |

* 1. Treści kształcenia (oddzielnie dla każdej formy zajęć)

Wykład

|  |  |
| --- | --- |
| Lp. | Treści kształcenia realizowane w ramach wykładów |
| W1 | Cyberprzestrzeń – aktorzy bezpieczeństwa, cyberprzestępcy, specjaliści bezpieczeństwa , wpływ zagrożeń na osoby, biznes, instytucje |
| W2 | Modele bezpieczeństwa i standardy. Podstawowe składowe: poufność, integralność, dostępność |
| W3 | Zagrożenia i podatności – przegląd |
| W4 | Zapewnienie poufności – kryptografia. Techniki, narzędzia, protokoły |
| W5 | Zapewnienie integralności. Metody kontroli integralności, podpis cyfrowy, certyfikaty. Integralność w bazach danych |
| W6 | Wysoka dostępność i niezawodność. Metody podnoszenia niezawodności, reagowanie na incydenty, odzyskiwanie po awarii |
| W7 | Zabezpieczanie urządzeń i systemów. Zabezpieczenie serwerów, sieci. Bezpieczeństwo fizyczne |

Laboratorium

|  |  |
| --- | --- |
| Lp. | Treści kształcenia realizowane w ramach laboratorium |
| L1 | Identyfikacja zagrożeń z wykorzystaniem profesjonalnych baz. Przygotowanie środowiska w oparciu o wirtualizację |
| L2 | Stosowanie metod uwierzytelnienia, autoryzacji i ewidencjonowania w systemach operacyjnych |
| L3 | Wykrywanie podstawowych zagrożeń w systemie operacyjnym |
| L4 | Szyfrowanie i łamanie haseł |
| L5 | Badanie podpisów cyfrowych. Konfigurowanie bezpiecznego zdalnego dostępu |
| L6 | Zabezpieczanie systemu operacyjnego |

Projekt

|  |  |
| --- | --- |
| Lp. | Treści kształcenia realizowane w ramach projektu |
| P1 | Analiza zagrożenia. Zapoznanie się z opisami w bazach danych zagrożeń |
| P2 | Planowanie środków zaradczych dotyczących wybranego zagrożenia |
| P3 | Przygotowanie eksperymentu weryfikującego skuteczność ochrony |
| P4 | Wnioski |

* 1. Korelacja pomiędzy efektami uczenia się, celami przedmiotu, a treściami kształcenia

|  |  |  |
| --- | --- | --- |
| Efekt uczenia się | Cele przedmiotu | Treści kształcenia |
| P\_W01 | C1 | W1-W7 |
| P\_W02 |
| P\_U01 | P1-P4 |
| P\_U02 |
| P\_U03 | L1-L6 |

* 1. Metody weryfikacji efektów uczenia się

|  |  |  |
| --- | --- | --- |
| Efekt  uczenia się | Metoda oceny | Forma zajęć, w ramach której następuje weryfikacja efektu |
| P\_W01 | Pytania otwarte | Wykład |
| P\_W02 |
| P\_U01 | Prezentacja projektu | Projekt |
| P\_U02 | Ocena projektu |
| P\_U03 | Ocena wykonania poszczególnych laboratoriów | laboratorium |

* 1. Kryteria oceny stopnia osiągnięcia efektów uczenia się

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Efekt uczenia się | Na ocenę 2  student nie potrafi | Na ocenę 3  student potrafi | Na ocenę 4  student potrafi | Na ocenę 5  student potrafi |
| P\_W01 | Wykazać się wiedzą z zakresu podstawowych technik bezpieczeństwa oraz przeciwdziałania zagrożeniom | Odpowiada poprawnie na co najmniej 50% pytań z zakresu podstawowych technik bezpieczeństwa oraz przeciwdziałania zagrożeniom | Odpowiada poprawnie na co najmniej 70% pytań z zakresu podstawowych technik bezpieczeństwa oraz przeciwdziałania zagrożeniom | Odpowiada poprawnie na co najmniej 85% pytań z zakresu podstawowych technik bezpieczeństwa oraz przeciwdziałania zagrożeniom |
| P\_W02 | Wykazać się zrozumieniem źródeł zagrożeń podczas stosowania technologii IT i ich zależności ekonomicznych, prawnych i etycznych | Odpowiada poprawnie na co najmniej 50% pytań z zakresu stosowania technologii IT i ich zależności ekonomiczne, prawne i etyczne | Odpowiada poprawnie na co najmniej 70% pytań z zakresu stosowania technologii IT i ich zależności ekonomiczne, prawne i etyczne | Odpowiada poprawnie na co najmniej 85% pytań z zakresu stosowania technologii IT i ich zależności ekonomiczne, prawne i etyczne |
| P\_U01 | Potrafi przedstawić w formie prezentacji wyników realizacji projektu | Potrafi przedstawić w formie prezentacji wyniki realizacji projektu – kluczowe elementy, z mnie znaczącymi błędami lub brakami | Potrafi przedstawić w formie prezentacji wyniki realizacji projektu – kluczowe elementy, brak błędów i braków | Potrafi przedstawić w formie prezentacji wyniki realizacji projektu – duża szczegółowość i wysoka jakość przekazu |
| P\_U02 | Potrafi zidentyfikować zagrożenia, zbadać jego działania i opracować środków zaradczych | Potrafi zidentyfikować zagrożenie, zbadać jego działanie i opracować środki zaradcze – zrealizowane wszystkie wymagane działania w zakresie dostatecznym | Potrafi zidentyfikować zagrożenie, zbadać jego działanie i opracować środki zaradcze – zrealizowane wszystkie wymagane działania w zakresie dobrym | Potrafi zidentyfikować zagrożenie, zbadać jego działanie i opracować środki zaradcze – zrealizowane wszystkie wymagane działania w sposób wyróżniający |
| P\_U03 | Posługiwać się technikami, narzędziami i oprogramowaniem w celu badania zagrożeń i ich przeciwdziałaniu | Posługuje się technikami, narzędziami i oprogramowaniem w celu badania zagrożeń i ich przeciwdziałaniu – wykonał poprawnie 70% ćwiczeń | Posługuje się technikami, narzędziami i oprogramowaniem w celu badania zagrożeń i ich przeciwdziałaniu – wykonał poprawnie 85% ćwiczeń | Posługuje się technikami, narzędziami i oprogramowaniem w celu badania zagrożeń i ich przeciwdziałaniu – wykonał poprawnie wszystkie ćwiczenia |

* 1. Literatura

|  |
| --- |
| Literatura podstawowa |
| <http://netacad.com> – Cybersecurity Essentials |
| Dr. Erdal Ozkaya, Cybersecurity: A comprehensive guide to getting started in cybersecurity, Packt Publishing, 2019 or newer |
| Yuri Diogenes, Erdal Ozkaya, Cybersecurity – Attack and Defense Strategies: Counter modern threats and employ state-of-the-art tools and techniques to protect your organization against cybercriminals, 2nd Edition Paperback – December 31, Packt Publishing, 2019 or newer |

|  |
| --- |
| Literatura uzupełniająca |
| Brian Walker, Cyber Security: Comprehensive Beginners Guide to Learn the Basics and Effective Methods of Cyber Security, 2019 |
| Henry George, Cybersecurity: Essential Guide for Beginners to Learn Basic Methods of Cybersecurity, 2020 |

1. Nakład pracy studenta - bilans punktów ECTS

|  |  |
| --- | --- |
| **Rodzaje aktywności** | **Obciążenie studenta** |
| **studia ST** |
| Udział w W/K (UB) | 14 |
| Konsultacje do W/K (UB) | 5 |
| Udział w egzaminie z W (UB) | 2 |
| Samodzielne studiowanie tematyki W/K, w tym przygotowanie do egzaminu/zaliczenia | 23 |
| Udział w C/L (UB) | 14 |
| Konsultacje do C/L (UB) | 5 |
| Samodzielne przygotowanie się do C/L, w tym przygotowanie do zaliczenia | 23 |
| Udział w i konsultacje do PS/PN/eL (UB) | 24 |
| Samodzielne przygotowanie się do zaliczenia PS/PN/eL | 43 |
| **Sumaryczne obciążenie pracą studenta** | **153** |
| **Punkty ECTS za przedmiot** | **6** |
| **Punkty ECTS za zajęcia prowadzone z bezpośrednim udziałem nauczycieli i studentów (UB)** | **3** |
| **Punkty ECTS za zajęcia kształtujące umiejętności praktyczne (PZ)** | **5** |