**karta przedmiotu**

1. Podstawowe informacje o przedmiocie

|  |  |
| --- | --- |
| Nazwa przedmiotu | Bezpieczeństwo w sieciach IoT |
| Rocznik studiów | 2022/2023 |
| Kolegium | Informatyki Stosowanej |
| Kierunek studiów | Informatyka |
| Poziom kształcenia | Studia pierwszego stopnia - inżynierskie |
| Profil kształcenia | Praktyczny |
| Specjalność | Technologie IoT (Internetu Rzeczy) |
| Osoba odpowiedzialna | dr inż. Janusz Korniak |

1. Wymagania wstępne (wynikające z następstwa przedmiotów)

|  |
| --- |
| Brak |

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

|  |  |
| --- | --- |
| C1 | Przekazanie wiedzy z zakresu bezpieczeństwa systemów Internetu Rzeczy |
| C2 | Kształcenie umiejętności ewaluacji podatności systemu IoT |
| C3 | Kształcenie umiejętności planowania eksperymentu |

* 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 | Potrafi omówić problemy bezpieczeństwa systemów IoT | K\_W09 |
| P\_W02 | Zna elementy (protokoły, rozwiązania, standardy) związane ze stosowaniem środków bezpieczeństwa i ewaluacją poziomu bezpieczeństwa | K\_W04 |
| Po zaliczeniu przedmiotu student w zakresie **umiejętności** | | |
| P\_U01 | Potrafi przeprowadzić eksperyment ewaluacji podatności systemu IoT | K\_U18 |
| P\_U02 | Potrafi samodzielnie przygotować i zaplanować eksperyment badania podatności systemów | K\_U02, K\_U12 |
| P\_U03 | Potrafi analizować informacje o podatnościach i ocenić zagrożenie | K\_U21 |
| Po zaliczeniu przedmiotu student w zakresie **kompetencji społecznych** | | |
| P\_K01 | Aktywnie komunikuje się w zakresie realizowanych zadań z otoczeniem | K\_K06 |

* 1. Formy zajęć dydaktycznych oraz wymiar godzin i punktów ECTS (w tabeli wyróżniono zajęcia kształtujące umiejętności praktyczne)

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Studia stacjonarne (ST) | | | | | | | |
| W | K | Ćw | L | ZP | P | eL | ECTS |
| - | - | - | 30 | - | 20 | - | 5 |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Studia niestacjonarne (NST) | | | | | | | |
| W | K | Ćw | L | ZP | P | eL | ECTS |
| - | - | - | 20 | - | 20 | - | 5 |

* 1. Metody realizacji zajęć dydaktycznych

|  |  |
| --- | --- |
| Formy zajęć | Metoda realizacji |
| Laboratorium | Zajęcia polegające na wykonywaniu eksperymentów związanych z bezpieczeństwem systemów IoT odzwierciedlających rzeczywiste warunki. 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 systemów IoT. |
| Projekt | Zajęcia polegają na analizie aktualnych zagrożeń w systemach IoT oraz zaplanowaniu eksperymentu mającego za zadanie badanie potencjalnych podatności systemu. |

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

Laboratorium

|  |  |
| --- | --- |
| Lp. | Treści kształcenia realizowane w ramach laboratorium |
| L1 | Ewaluacja zagrożeń w systemach IoT do zastosowań domowych i przemysłowych |
| L2 | Przygotowanie środowiska IoT na bazie Raspberry Pi |
| L3 | Zabezpieczanie systemy IoT |
| L4 | Przygotowanie narzędzi ewaluacji bezpieczeństwa |
| L5 | Badanie podatności systemu IoT |

Projekt

|  |  |
| --- | --- |
| Lp. | Treści kształcenia realizowane w ramach wykładów |
| P1 | Analiza problemów bezpieczeństwa IoT  Analiza wymagań bezpieczeństwa systemów IoT oraz modeli i standardów  Analiza podatności bezpieczeństwa urządzeń fizycznych w systemach IoT  Podatności bezpieczeństwa komunikacji w systemach IoT  Analiza bezpieczeństwa aplikacji i usług IoT  Zarządzanie ryzykiem |
| P2 | Planowanie eksperymentu, projekt i plan działania |
| P3 | Dokumentowanie i współpraca w działaniach projektowych |

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

|  |  |  |
| --- | --- | --- |
| Efekt uczenia się | Cele przedmiotu | Treści kształcenia |
| P\_W01 | C1 | P1 |
| P\_W02 | P1 |
| P\_U01 | C2 | L1 - L5 |
| P\_U02 | C3 | P2 |
| P\_U03 | C1 | P1 |
| P\_K01 | C3 | P3 |

* 1. Metody weryfikacji efektów uczenia się

|  |  |  |
| --- | --- | --- |
| Efekt  uczenia się | Metoda oceny | Forma zajęć, w ramach której następuje weryfikacja efektu |
| P\_W01 | Test wiedzy | Projekt |
| P\_W02 |
| P\_U01 | Weryfikacja wykonanych ćwiczeń | Laboratorium |
| P\_U02 | Ocena projektu | Projekt |
| P\_U03 | Ocena projektu | Projekt |
| P\_K01 | Ocena postawy i komunikacji podczas konsultacji | Projekt |

* 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 | Omówić problemów bezpieczeństwa systemów IoT | Przygotować opracowanie dotyczące wybranego problemu bezpieczeństwa systemów IoT – w zakresie podstawowym | Przygotować opracowanie dotyczące wybranego problemu bezpieczeństwa systemów IoT - w zakresie rozszerzonym | Przygotować opracowanie dotyczące wybranego problemu bezpieczeństwa systemów IoT - w zakresie szczegółowym |
| P\_W02 | Omówić elementów (protokoły, rozwiązania, standardy) związanych ze stosowaniem środków bezpieczeństwa i ewaluacją poziomu bezpieczeństwa | Przygotować opracowanie dotyczące wybranego elementu związanego ze stosowaniem środków bezpieczeństwa i ewaluacją poziomu bezpieczeństwa – w zakresie podstawowym | Przygotować opracowanie dotyczące wybranego elementu związanego ze stosowaniem środków bezpieczeństwa i ewaluacją poziomu bezpieczeństwa - w zakresie rozszerzonym | Przygotować opracowanie dotyczące wybranego elementu związanego ze stosowaniem środków bezpieczeństwa i ewaluacją poziomu bezpieczeństwa - w zakresie szczegółowym |
| P\_U01 | Przeprowadzić eksperyment podatności systemu IoT | Wykonać podstawowy zestaw eksperymentów | Wykonać wszystkie eksperymenty z mniej istotnymi błędami | Wykonać bezbłędnie wszystkie eksperymenty |
| P\_U02 | Potrafi samodzielnie przygotować i zaplanować eksperymentu badania podatności systemów | Potrafi przygotować i zaplanować eksperyment (o małej złożoności) badania podatności systemów z nieznaczną pomocą popełniając mniej znaczące błędy | Potrafi przygotować i zaplanować eksperyment (o małej złożoności) badania podatności systemów bez pomocy nie popełniając błędów | Potrafi przygotować i zaplanować eksperyment (o większej złożoności) badania podatności systemów bez pomocy nie istotnych popełniając błędów |
| P\_U03 | Potrafi analizować informacji o podatnościach ani ocenić zagrożenia | Przygotował analizę jednej podatności i potencjalnych zagrożeń | Przygotował analizę dwóch podatności i potencjalnych zagrożeń | Przygotował głębszą analizę dwóch podatności i potencjalnych zagrożeń |
| P\_K01 | Aktywnie komunikować się w zakresie realizowanych zadań z otoczeniem | Komunikuje się w zakresie realizowanych zadań z otoczeniem w stopniu dostatecznym dla zrozumienia realizowanych zadań | Komunikuje się w zakresie realizowanych zadań z otoczeniem w stopniu dobrym dla zrozumienia realizowanych zadań | Komunikuje się w zakresie realizowanych zadań z otoczeniem w stopniu bardzo dobrym dla zrozumienia realizowanych zadań |

* 1. Literatura

|  |
| --- |
| Literatura podstawowa |
| Fotios Chantzis, Ioannis Stais, Paulino Calderon, Evangelos Deirmentzoglou i in., Hakowanie internetu rzeczy w praktyce. Przewodnik po skutecznych metodach atakowania IoT, Helion 2022 lub nowsze |
| W. Stallings, L. Brown: Bezpieczeństwo systemów informatycznych. Zasady i praktyka. Tom 1, Wyd. Helion, Gliwice 2019 lub nowsze lub ebookpoint.pl |
| W. Stallings, L. Brown: Bezpieczeństwo systemów informatycznych. Zasady i praktyka. Tom 2, Wyd. Helion, Gliwice 2019 lub nowsze lub ebookpoint.pl |

|  |
| --- |
| Literatura uzupełniająca |
| Ansari, Juned Ahmed: Kali Linux. Testy penetracyjne, Wyd. Helion, Gliwice 2017 lub nowsze |
| L. Brotherston, A. Berlin: Bezpieczeństwo defensywne. Podstawy i najlepsze praktyki, Wyd. Helion, Gliwice 2018 lub nowsze |

1. Nakład pracy studenta - bilans punktów ECTS

|  |  |  |
| --- | --- | --- |
| **Rodzaje aktywności** | **Obciążenie studenta** | |
| **studia ST** | **studia NST** |
| Udział w C/L (UB) | 30 | 20 |
| Konsultacje do C/L (UB) | 6 | 4 |
| Samodzielne przygotowanie się do C/L, w tym przygotowanie do zaliczenia | 39 | 51 |
| Udział w i konsultacje do PS/PN/eL (UB) | 20 | 20 |
| Samodzielne przygotowanie się do zaliczenia PS/PN/eL | 30 | 30 |
| **Sumaryczne obciążenie pracą studenta** | **125** | **125** |
| **Punkty ECTS za przedmiot** | **5** | **5** |
| **Punkty ECTS za zajęcia prowadzone z bezpośrednim udziałem nauczycieli i studentów (UB)** | **2** | **2** |
| **Punkty ECTS za zajęcia kształtujące umiejętności praktyczne (PZ)** | **5** | **5** |