# KARTA OPISU PRZEDMIOTU - SYLABUS

Nazwa przedmiotu
Bezpieczeństwo systemów IoT [S2Inf1E-CYB>IOT]

## Przedmiot

Kierunek studiów
Informatyka/Computing

Rok/Semestr
1/2

Studia w zakresie (specjalność)
Cyberbezpieczeństwo

Profil studiów
ogólnoakademicki

Poziom studiów
drugiego stopnia

Język oferowanego przedmiotu
angielski

Forma studiów
stacjonarne

Wymagalność
obligatoryjny

## Liczba godzin

Wykład
30

Laboratorium
30

Inne
0

Ćwiczenia
0

Projekty/seminaria
15

## Liczba punktów ECTS

6,00

## Koordynatorzy

dr hab. inż. Paweł Śniatała prof. PP
pawel.sniatala@put.poznan.pl

prof. dr hab. inż. Mariusz Głąbowski
mariusz.glabowski@put.poznan.pl

## Wykładowcy

## Wymagania wstępne

Student rozpoczynający ten przedmiot powinien posiadać podstawową wiedzę z zakresu elektroniki cyfrowej, mikrokontrolerów i mikroprocesorów. Powinien posiadać wiedzę pozwalającą mu na projektowanie i implementację programów komputerowych w wybranych językach programowania (np. C, Python). Powinien również posiadać umiejętność pozyskiwania informacji ze wskazanych źródeł oraz być gotowy do współpracy w zespole. W obszarze kompetencji społecznych musi prezentować postawy takie jak: uczciwość, odpowiedzialność, wytrwałość, ciekawość poznawcza, kreatywność, kultura osobista, szacunek dla innych ludzi.

## Cel przedmiotu

Przekazanie studentom wiedzy z zakresu szeroko rozumianego bezpieczeństwa IoT oraz metod i narzędzi służących do szacowania i kontroli ryzyka naruszenia poufności, integralności i dostępności danych. Kluczowe koncepcje bezpieczeństwa: poufność, uwierzytelnienie, integralność, kontrola dostępu, niezaprzeczalność i dostępność oraz najnowocześniejsze rozwiązania w zakresie bezpieczeństwa będą wzmacniane i badane. Zapoznanie studentów z zaawansowanymi metodami, technikami i narzędziami stosowanymi w rozwiązywaniu złożonych zadań inżynierskich w zakresie projektowania i utrzymania systemów i urządzeń IoT z naciskiem na bezpieczeństwo systemów i danych.

## Przedmiotowe efekty uczenia się

Wiedza:
student jest w stanie zrozumieć lub opanować bezpieczeństwo iot związane ze sprzętem, systemem i siecią.
student ma uporządkowaną i teoretycznie uzasadnioną wiedzę ogólną związaną z kluczowymi zagadnieniami w dziedzinie bezpieczeństwa iot. omówiony zostanie zarówno poziom urządzenia jak i systemu.
student posiada zaawansowaną, szczegółową wiedzę z zakresu integracji wybranych czujników z platformami sprzętowymi (raspberry pi, arduino) oraz posiada wiedzę na temat luk bezpieczeństwa związanych z analizowanymi systemami.
student posiada wiedzę na temat trendów rozwojowych i najważniejszych nowych osiągnięć informatyki i telekomunikacji w zakresie bezpieczeństwa iot.

Umiejętności:
student może uzyskać informacje na temat doboru sensorów do realizacji założonych funkcji systemów iot oraz urządzeń iot z punktu widzenia bezpieczeństwa. uzyskane informacje, student potrafi zintegrować, a następnie poddać krytycznej ocenie.
student potrafi zaplanować i przeprowadzić badania w zakresie pomiaru i testowania bezpieczeństwa urządzeń i systemów iot, zinterpretować uzyskane wyniki i wyciągnąć wnioski.
student potrafi zaimplementować lekkie algorytmy kryptograficzne na platfromach iot.
student potrafi wykorzystywać metody eksperymentalne do formułowania i rozwiązywania zadań inżynierskich oraz prostych problemów badawczych w obszarze bezpieczeństwa iot.
student potrafi integrować wiedzę z różnych dziedzin informatyki i telekomunikacji przy formułowaniu i rozwiązywaniu zadań inżynierskich związanych z projektowaniem i implementacją systemów iot z uwzględnieniem wymagań bezpieczeństwa.
student potrafi ocenić przydatność wykorzystania nowych rozwiązań sprzętowych i programowych do rozwiązywania zadań inżynierskich, polegających na budowie wydajnych, bezpiecznych systemów iot.

Kompetencje społeczne:
student rozumie, że systemy iot integrują wiele technologii, a wiedza i umiejętności z zakresu bezpieczeństwa iot bardzo szybko się dezaktualizują.
student rozumie znaczenie wykorzystania najnowszej wiedzy z zakresu iot w rozwiązywaniu problemów badawczych i praktycznych.
student ma świadomość konieczności profesjonalnego podejścia do rozwiązywania problemów z zakresu iot i ponoszenia odpowiedzialności za proponowane przez siebie projekty.

## Metody weryfikacji efektów uczenia się i kryteria oceny

Efekty uczenia się przedstawione wyżej weryfikowane są w następujący sposób:

Wiedza zdobyta podczas wykładu jest weryfikowana poprzez test ustny i/lub pisemny.
Zagadnienia testowe, na podstawie których opracowywane są pytania, przesyłane są do studentów drogą elektroniczną za pomocą uczelnianego systemu poczty elektronicznej.
Egzamin ustny i/lub pisemny składa się z 3 do 5 pytań, na które oczekuje się odpowiedzi opisowej. Każda odpowiedź na pytanie jest oceniana w skali od 0 do 5 punktów. Każde pytanie jest jednakowo punktowane. Próg zaliczenia: 50% punktów.
W przypadku egzaminu ustnego studenci losują pytania z zestawu 30 pytań. W przypadku sprawdzianu pisemnego pytania zadaje wykładowca.
Umiejętności nabyte podczas zajęć laboratoryjnych są weryfikowane na bieżąco. Na każdych zajęciach laboratoryjnych poprawność wykonania ćwiczeń oceniana jest w skali od 2 do 5. Ocena końcowa jest średnią ocen uzyskanych z poszczególnych zajęć laboratoryjnych. Ocena końcowa jest średnią ocen

uzyskanych z poszczególnych zajęć laboratoryjnych.

## Treści programowe

- Internet Rzeczy (IoT)
- Zasady bezpieczeństwa IoT.
- Studia przypadków cyberataków na systemy IoT.
- Przegląd wybranych platform sprzętowych IoT i środowiska programistycznego.
- Łączność / komunikacja urządzeń IoT.
- Lekkie algorytmy kryptograficzne.
- Cyfrowa kryminalistyka w IoT.

## Tematyka zajęć

Tematyka wykładów:
- Internet Rzeczy (IoT) - aplikacje, systemy, urządzenia, sensory.
- Zasady bezpieczeństwa IoT.
- Studia przypadków cyberataków na systemy IoT.
- Przegląd wybranych platform sprzętowych IoT i środowiska programistycznego (Raspberry Pi, Tizen) .
- Łączność / komunikacja urządzeń IoT (lekkie protokoły komunikacyjne IoT).
- Lekkie algorytmy kryptograficzne.
- Bezpieczeństwo systemów IoT i TustZone, Wykrywanie i zapobieganie włamaniom w IoT, Złośliwe oprogramowanie w IoT
- Cyfrowa kryminalistyka w IoT.

Zagadnienia laboratoryjne:
- Wykorzystanie Arduino do pozyskiwania informacji o parametrach środowiskowych (czujniki temperatury, fororezystory itp.)
- Awaryjne zatrzymanie procesu produkcyjnego w odpowiedzi na alarmy środowiskowe (Raspberry PI, JSON, MongoDB).
- Wykorzystanie Packet Tracer do testowania rozwiązań w dziedzinie inteligentnych miast i sieci (smart grids).
- Prototypowanie i testowanie instalacji inteligentnego domu przy użyciu Packet Tracer (Python, komputer jednopłytkowy, smartfon / tablet, router, czujnik otwarcia drzwi, itp.)
- Inteligentna kamera wrażliwa na uśmiech (Raspberry PI, kamera Raspberry PI, Python, uczenie maszynowe)
- Konfiguracja systemu zapobiegania włamaniom (Intrusion Prevention System - IPS).
- Testowanie podatności prostych rozwiązań IoT (Sensor-Actuator System, IFTTT) w zakresie bezpieczeństwa teleinformatycznego
- Implementacja wybranych lekkich algorytmów kryptograficznych (C, python).

Projekt:
Przygotowanie pracy naukowej w wybranej tematyce.

## Metody dydaktyczne

Wykłady: prezentacje multimedialne, ilustrowane przykładami podawanymi na tablicy.
Ćwiczenia laboratoryjne: ćwiczenia praktyczne w grupach z wykorzystaniem platform sprzętowych.

## Literatura

Podstawowa
1. Paweł Śniatała, Sitharama S Iyengar, Sanjeev Kaushik Ramani: Evolution of Smart Sensing Ecosystems and the need for Tamper Evident Security: Theory to Practice. Springer 2021
2. William Stallings, Lawrie Brown: Computer Security, Principles and Practice, Pearson 2015. ISBN: 0-13-377392-2.
3. Gaston C. Hillar, Internet of Things with Python Paperback, Packt Publishing, 2016.
Uzupełniająca
1. Marcin Sikorski, Adam Roman: Internet Rzeczy, Wydawnictwo Naukowe PWN 2020. ISBN: 9788301208400

## Bilans nakładu pracy przeciętnego studenta

| | Godzin | ECTS |
|---|---|---|
| Łączny nakład pracy | 150 | 6,00 |
| Zajęcia wymagające bezpośredniego kontaktu z nauczycielem | 75 | 3,00 |
| Praca własna studenta (studia literaturowe, przygotowanie do zajęć laboratoryjnych/ćwiczeń, przygotowanie do kolokwiów/egzaminu, wykonanie projektu) | 75 | 3,00 |