



UNIwersYTET
IM. ADAMA MICKIEWICZA
W POZNANIU

Bezpieczeństwo w ekosystemie IoT

Sylabus zajęć

Informacje podstawowe

Kierunek studiów Informatyka Specjalność - Jednostka organizacyjna Wydział Matematyki i Informatyki Poziom studiów studia inżynierskie pierwszego stopnia Forma studiów studia niestacjonarne Profil studiów profil ogólnoakademicki		Cykl dydaktyczny 2023/24 Kod zajęć 06INFN.320S.03132.23 Języki wykładowe polski Obligatoryjność Fakultatywny Blok zajęciowy Przedmioty specjalnościowe
Koordynator zajęć	Tomasz Kowalski	
Prowadzący zajęcia	Tomasz Kowalski	
Okres Semestr 6	Forma zajęć / liczba godzin / forma zaliczenia - Wykład: 15, Egzamin - Laboratorium: 15, Zaliczenie z oceną	Liczba punktów ECTS 5

Cele kształcenia dla zajęć

Kod	Cel
C1	Wskazanie specyficznych dla IoT wyzwań, mechanizmów i technik zapewnienia bezpieczeństwa.
C2	Wskazanie aktualnych kierunków prac badawczo-rozwojowych mających na celu poprawę bezpieczeństwa.

Wymagania wstępne

Podstawowa wiedza w zakresie budowy i działania systemu operacyjnego, sieci komputerowej i architektury aplikacji.
Podstawowa wiedza w zakresie działania i budowy produktów lub rozwiązań IoT (np. dla tzw. inteligentnego domu).

Efekty uczenia się dla zajęć

Kod	Efekty uczenia się dla zajęć w zakresie	Efekty uczenia się dla kierunku	Metody weryfikacji osiągnięcia efektów uczenia się dla zajęć
Wiedzy - Student/ka:			
W1	Ma świadomość trudności w skalowaniu praktyk bezpieczeństwa w dół - do ograniczonych urządzeń.	INF_K3_W03, INF_K3_W04_inz, INF_K3_W06_inz, INF_K3_W07	Egzamin pisemny
W2	Zna sprzętowe technologie wspierające bezpieczeństwo.	INF_K3_W03, INF_K3_W06_inz, INF_K3_W07	Egzamin pisemny
Umiejętności - Student/ka:			
U1	Potrafi dobrać i zastosować środowisko ramowe w projekcie informatycznym.	INF_K3_U05_inz, INF_K3_U06_inz	Projekt, Raport
U2	Potrafi dobrać i zastosować w projekcie wspierane sprzętowo mechanizmy bezpieczeństwa.	INF_K3_U05_inz, INF_K3_U06_inz	Projekt, Raport
U3	Potrafi dobrać i zastosować w projekcie właściwe mechanizmy łączności sieciowej.	INF_K3_U05_inz, INF_K3_U06_inz	Projekt, Raport
Kompetencji społecznych - Student/ka:			
K1	Jest gotów/gotowa do identyfikacji zagrożeń i podejmowania środków zaradczych w zależności do gałęzi przemysłu, dla której realizowany jest projekt.	INF_K3_K03, INF_K3_K06	Egzamin pisemny

Treści programowe dla zajęć

Lp.	Treści programowe dla zajęć	Efekty uczenia się dla zajęć	Formy zajęć
1.	Kompromisy w zakresie bezpieczeństwa. Konsekwencje decyzji projektowych mających na celu minimalizację kosztu urządzenia.	W1, K1	Wykład, Laboratorium
2.	Środowiska ramowe dla IoT. Architektura. Standardy konsumenckie. Standardy przemysłowe. Zagadnienia zapewnienia łączności, zarządzalności, rozproszonego wdrożenia aplikacji. Trudności wokół interoperacyjności.	W1, U1, K1	Wykład, Laboratorium
3.	Komponenty sprzętowe w budowaniu bezpieczeństwa. Zasadnicze środki ochronne dla przechowywania, inicjalizacji i wykonania. Znaczenie sprzętu w odbudowywaniu czystego systemu.	W1, W2, K1	Wykład, Laboratorium
4.	Komponenty programowe w budowaniu bezpieczeństwa. Wpływ możliwości sprzętowych na kształt oprogramowania. Rola systemu operacyjnego w budowaniu bezpiecznych rozwiązań.	W1, U2, K1	Wykład, Laboratorium
5.	Technologie łączności w IoT. Zagadnienia przewodowej komunikacji w czasie rzeczywistym. Uwagi dot. wybranych technologii bezprzewodowych.	W1, W2, U3, K1	Wykład, Laboratorium

Lp.	Treści programowe dla zajęć	Efekty uczenia się dla zajęć	Formy zajęć
6.	Wyzwania w tzw. aplikacjach pionowych. Wymagania bezpieczeństwa specyficzne dla gałęzi przemysłu. O konieczności wspólnych sprzętowych i programowych elementów konstrukcyjnych.	W1, K1	Wykład, Laboratorium

Informacje dodatkowe

Forma zajęć	Metody i formy prowadzenia zajęć
Wykład	Wykład z prezentacją multimedialną wybranych zagadnień, Wykład konwersatoryjny
Laboratorium	Metoda laboratoryjna, Metoda projektu

Forma zajęć	Warunki zaliczenia zajęć
Wykład	Warunkiem uzyskania pozytywnej oceny jest uzyskanie zaliczenia z laboratoriów. Wynik egzaminu przekłada się na końcową ocenę w następujący sposób: 1. bardzo dobry (bdb; 5,0) – od 90% punktów, 2. dobry plus (db plus; 4,5) – od 80% punktów, 3. dobry (db; 4,0) – od 70% punktów, 4. dostateczny plus (dst plus; 3,5) – od 60% punktów, 5. dostateczny (dst; 3,0) – od 50% punktów, 6. niedostateczny (ndst; 2,0) – poniżej 50% punktów.
Laboratorium	Na końcową ocenę składają się wyniki uzyskane z mikroprojektów i raportów. Skala ocen: 1. bardzo dobry (bdb; 5,0) – od 90% punktów, 2. dobry plus (db plus; 4,5) – od 80% punktów, 3. dobry (db; 4,0) – od 70% punktów, 4. dostateczny plus (dst plus; 3,5) – od 60% punktów, 5. dostateczny (dst; 3,0) – od 50% punktów, 6. niedostateczny (ndst; 2,0) – poniżej 50% punktów.

Literatura

Obowiązkowa

1. Fotios Chantzis, Ioannis Stais, "Practical IoT Hacking", 2021
2. Perry Lea, "IoT and Edge Computing for Architects", 2020
3. Keith Gremban, Ananthram Swami, "IoT for Defense and National Security", 2023
4. Brian Russell, Drew Van Duren, "Practical Internet of Things Security", 2016
5. Alasdair Gilchrist, "IoT Security Issues", 2017

Nakład pracy studenta i punkty ECTS

Rodzaje zajęć studenta	Średnia liczba godzin* przeznaczonych na zrealizowane rodzaje zajęć
Wykład	15
Laboratorium	15
Przygotowanie projektu	40

Przygotowanie raportu	15
Przygotowanie do egzaminu	10
Czytanie wskazanej literatury	30
Łączny nakład pracy studenta	Liczba godzin 125
Liczba punktów ECTS	ECTS 5

* godzina (lekcyjna) oznacza 45 minut

Efekty uczenia się dla kierunku

Kod	Treść
INF_K3_K03	Absolwent/ka jest gotów/gotowa do pełnienia roli zawodowej informatyka ze świadomością ciągłych zmian stosowanych paradygmatów i technologii
INF_K3_K06	Absolwent/ka jest gotów/gotowa do uczestniczenia w procesach gospodarczych związanych z informatyką i świadczeniem wybranych usług informatycznych
INF_K3_U05_inz	Absolwent/ka potrafi pisać, uruchamiać i testować programy w wybranym środowisku programistycznym
INF_K3_U06_inz	Absolwent/ka potrafi ocenić, na podstawowym poziomie, przydatność metod i narzędzi informatycznych oraz wybrać i zastosować właściwą metodę i narzędzia do typowych zadań informatycznych
INF_K3_W03	Absolwent/ka zna i rozumie narzędzia, technologie i urządzenia informatyczne właściwe dla wybranych obszarów zastosowań oraz podstawy ich działania
INF_K3_W04_inz	Absolwent/ka zna i rozumie zaawansowane pojęcia, konstrukcje i procesy związane z językami programowania i inżynierią programowania
INF_K3_W06_inz	Absolwent/ka zna i rozumie zaawansowane pojęcia związane z informatyczną architekturą sprzętowo-programową
INF_K3_W07	Absolwent/ka zna i rozumie zaawansowane pojęcia związane z technologiami sieciowymi, bezpieczeństwem i protokołami kryptograficznymi