KARTA OPISU PRZEDMIOTU - SYLABUS

Nazwa przedmiotu

Bezpieczeństwo przemysłowego Internetu Rzeczy

Przedmiot

Kierunek studiów

Informatyka

Rok/semestr

1/2

Studia w zakresie (specjalność)

Cyberbezpieczeństwo

Profil studiów

ogólnoakademicki

Poziom studiów

drugiego stopnia

Język oferowanego przedmiotu

angielski

Forma studiów

stacjonarne

Wymagalność

obieralny

Liczba godzin

Wykład

15

Laboratoria

15

Inne (np. online)

Ćwiczenia

Projekty/seminaria

Liczba punktów ECTS

2

Wykładowcy

Odpowiedzialny za przedmiot/wykładowca:

dr inż. Maciej Sobieraj

maciej.sobieraj@put.poznan.pl

tel: 61 665 3909

Wydział Informatyki i Telekomunikacji

Polanka 3, 60-965 Poznań

Odpowiedzialny za przedmiot/wykładowca:

mgr inż. Michał Weissenberg

email: michal.weissenberg@put.poznan.pl

tel: 51 665 3946

Wydział Informatyki i Telekomunikacji

Polanka 3, 60-965 Poznań

Wymagania wstępne

Student rozpoczynający ten kurs powinien posiadać podstawową wiedzę z zakresu cyberbezpieczeństwa i IoT. Ponadto student powinien posiadać podstawową wiedzę o sieciach teleinformatycznych, podstawowe umiejętności konfiguracji urządzeń sieciowych oraz rozumieć proces komunikacji pomiędzy urządzeniami sieciowymi. Student powinien ponadto posiadać podstawowe umiejętności programowania. Student powinien również posiadać umiejętność pozyskiwania informacji ze wskazanych źródeł.

Student powinien wykazywać takie cechy jak uczciwość, odpowiedzialność, wytrwałość, ciekawość poznawcza, kreatywność, kultura osobista, szacunek dla drugiego człowieka oraz gotowość do pracy w grupie.

Cel przedmiotu

1. Zapewnienie studentom teoretycznych podstaw dotyczących architektury Przemysłowego Internetu Rzeczy, jego komponentów i aplikacji.

2. Zapoznanie studentów z wymaganiami teoretycznymi i praktycznymi dotyczącymi bezpieczeństwa poszczególnych warstwach sieci od jej brzegu do rdzenia.

3. Zapoznanie studentów ze standardami i regulacjami dotyczącymi wymagań audytowych oraz protokołów, aplikacji i IPv6 dla IIoT.

4. Przedstawienie zagadnień pozwalających na identyfikację podatności i zagrożeń w IIoT.

5. Przedstawienie najlepszych praktyk w zakresie zasad projektowania oraz procesu zabezpieczania i segmentacji sieci IIoT.

Przedmiotowe efekty uczenia się

Wiedza

Student ma zaawansowaną i pogłębioną wiedzę z zakresu szeroko rozumianych metod tworzenia sieci IIoT, teoretycznych podstaw ich budowy oraz wykorzystania narzędzi do zarządzania nimi.

Student zna trendy oraz najważniejsze i najnowsze osiągnięcia w sieciach teleinformatycznych, a przede wszystkim w obszarze zabezpieczania infrastruktury krytycznej i sieci IIoT.

Student zna zaawansowane metody, techniki i narzędzia stosowane do rozwiązywania złożonych problemów w zabezpieczaniu sieci IIoT oraz potrafi wykorzystywać protokoły i funkcje zapewniające bezpieczeństwo systemu na urządzeniach sieciowych i urządzeniach IIoT.

Student posiada bogate słownictwo w języku angielskim z zakresu terminologii stosowanej w tematach związanych z Przemysłowym Internetem Rzeczy.

Umiejętności

Student potrafi się kształcić się samodzielnie, zdobywając wiedzę niezbędną do zrozumienia i rozwiązywania problemów występujących w obszarze zabezpieczenia Przemysłowego Internetu Rzeczy.

Student potrafi pracować w grupie, aktywnie uczestnicząc w planowaniu kursu i realizacji zajęć laboratoryjnych związanych z bezpieczeństwem Przemysłowego Internetu Rzeczy.

Student potrafi ocenić przydatność i możliwość wykorzystania nowych osiągnięć (protokołów i narzędzi) w urządzeniach IIoT i urządzeniach sieciowych do zabezpieczenia systemu Przemysłowego Internetu Rzeczy.

Student potrafi wykrywać podatności w sieciach IIoT i je eliminować.

Kompetencje społeczne

Student ma świadomość postępu i wynikającej z niego potrzeby ciągłego dokształcania się w zakresie bezpieczeństwa Przemysłowego Internetu Rzeczy.

Student ma świadomość odpowiedzialności za wspólną pracę w zespołach realizujących projekty teleinformatyczne.

Student ma świadomość odpowiedzialności za wyniki swojej pracy, co ma bezpośredni wpływ na bezpieczeństwo ludzi i urządzeń składających się na Przemysłowy Internet Rzeczy.

Metody weryfikacji efektów uczenia się i kryteria oceny

Efekty uczenia się przedstawione wyżej weryfikowane są w następujący sposób:

Wykład: wiedza jest weryfikowana poprzez test pisemny i/lub ustny. Ocena zaliczeniowa wynosi 51% punktów, a podczas egzaminu nie wolno używać żadnych materiałów pomocniczych.

Laboratoria: wiedza i umiejętności są weryfikowane na podstawie oceny bieżącego postępu w realizacji zadań; sprawdzenie zakładanych efektów uczenia się odbywa się poprzez ewaluację. Pisemne raporty dotyczące poszczególnych tematów laboratoryjnych oraz praktyczne testy umiejętności konfigurowania bezpiecznych systemów IIoT.

Treści programowe

Wykład:

1. Wprowadzenie - pojęcia, definicje, historia i charakterystyka architektury sieci Industrial IoT.

2. Wymagania bezpieczeństwa - wprowadzenie do wymagań bezpieczeństwa sieci Przemysłowego IoT.

3. Protokoły - najważniejsze informacje o protokołach wykorzystywanych w sieciach Przemysłowego IoT.

4. Podatności - analiza podatności i zapobieganie im w sieciach IIoT.

5. Zabezpieczanie - prezentacja i realizacja procesu zabezpieczania sieci IIoT.

6. Securing - prezentacja i implementacja zaawansowanych funkcji bezpieczeństwa służących do zabezpieczania sieci IIoT.

7. VPN - opis i implementacja rozwiązań VPN w sieciach IIoT.

8. Rozwiązania komercyjne - prezentacja rozwiązań komercyjnych w zakresie bezpieczeństwa sieci IIoT.

Laboratorium:

1. Wstęp

2. Przegląd środowiska symulacyjnego i urządzeń fizycznych

3. Zrozumieć działania elementów sieci Przemysłowego IoT i określenie wymagań dotyczące bezpieczeństwa

4. Analiza ruchu sieciowego warstwy 2 i warstwy 3 w sieci Przemysłowego IoT

5. Analiza zasobów i wykrywanie podatności w sieci IIoT

6. Poznawanie komercyjnych rozwiązań bezpieczeństwa infrastruktury sieciowej w sieci IIoT

7. Zarządzanie cyklem życia IIoT

Metody dydaktyczne

1. Wykład: prezentacja multimedialna ilustrowana przykładami.

2. Ćwiczenia laboratoryjne: wykonywanie zadań zleconych przez prowadzącego – ćwiczenia praktyczne, praca zespołowa,korzystanie z urządzeń sieciowych i środowisk symulacyjnych.

Literatura

Podstawowa

Literatura z uznanych czasopism naukowych, dokumenty normalizacyjne, strony internetowe producentów urządzeń umieszczane przez prowadzącego na platformie ekursy.

Kursy i materiały przygotowane przez producentów sprzętu.

Uzupełniająca

Bilans nakładu pracy przeciętnego studenta

	Godzin	ECTS
Łączny nakład pracy	50	2,0
Zajęcia wymagające bezpośredniego kontaktu z nauczycielem	30	1,5
Praca własna studenta (studia literaturowe, przygotowanie do zajęć laboratoryjnych, przygotowanie do zadań praktycznych na laboratoriach oraz egzaminu)[1]	20	0,5

[1] niepotrzebne skreślić lub dopisać inne czynności