KARTA OPISU PRZEDMIOTU - SYLABUS

Nazwa przedmiotu
Bezpieczeństwo systemów IoT i IIoT [S1Cybez1>BSIoT]

Przedmiot

Kierunek studiów
Cyberbezpieczeństwo

Rok/Semestr
3/5

Studia w zakresie (specjalność)
–

Profil studiów
ogólnoakademicki

Poziom studiów
pierwszego stopnia

Język oferowanego przedmiotu
polski

Forma studiów
stacjonarne

Wymagalność
obieralny

Liczba godzin

Wykład
24

Laboratorium
16

Inne
0

Ćwiczenia
0

Projekty/seminaria
16

Liczba punktów ECTS

4,00

Koordynatorzy

dr hab. inż. Maciej Sobieraj
maciej.sobieraj@put.poznan.pl

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

Wykładowcy

Wymagania wstępne

Podstawy lokalnych i rozległych sieci komputerowych oraz systemów IoT.

Cel przedmiotu

• Zapoznanie studentów z kluczowymi zagadnieniami bezpieczeństwa IoT i IIoT. • Rozwinięcie umiejętności projektowania i zabezpieczania systemów IoT i IIoT. • Zrozumienie specyfiki bezpieczeństwa w środowiskach przemysłowych, w tym infrastruktury krytycznej. • Przygotowanie studentów do pracy w zespołach zajmujących się bezpieczeństwem systemów IoT i IIoT

Przedmiotowe efekty uczenia się

Wiedza:
• Student zna podstawowe zagadnienia związane z bezpieczeństwem IoT i IIoT. [K1_W10]
• Rozumie modele bezpieczeństwa stosowane w przemyśle (np. Model Purdue). [K1_W10]
• Zna zasady zarządzania cyklem życia systemów IoT i IIoT. [K1_W09]

Umiejętności:
• Potrafi zaprojektować i wdrożyć zabezpieczenia systemów IoT i IIoT. [K1_U02]
• Umie analizować zagrożenia i wdrażać mechanizmy ochrony w systemach przemysłowych. [K1_U09]
• Stosuje narzędzia do monitorowania i automatyzacji w środowiskach IoT i IIoT. [K1_U04]

Kompetencje społeczne:
• Rozumie znaczenie ochrony infrastruktury krytycznej w środowiskach przemysłowych. [K1_K01]
• Jest świadomy konieczności ciągłego doskonalenia wiedzy w dynamicznie rozwijającym się obszarze IoT i IIoT.[K1_K05]

Metody weryfikacji efektów uczenia się i kryteria oceny

Efekty uczenia się przedstawione wyżej weryfikowane są w następujący sposób:

Efekty uczenia się przedstawione wyżej weryfikowane są w następujący sposób:
1. Wiedza: egzamin pisemny obejmujący zagadnienia bezpieczeństwa IoT i IIoT.
2. Umiejętności: bieżąca ocena zadań laboratoryjnych oraz ocena końcowa projektu grupowego.
W każdej formie zaliczenia przedmiotu ocena zależy od liczby zdobytych przez studenta punktów w stosunku do maksymalnej liczby punktów obowiązkowych. Warunkiem pozytywnego zaliczenia jest otrzymanie co najmniej 50% punktów możliwych do zdobycia. Zależność oceny od liczby punktów definiuje Regulamin Studiów. Dodatkowo zasady zaliczania przedmiotu i dokładne progi zaliczeniowe zostaną przekazane studentom na początku semestru z wykorzystaniem uczelnianych systemów elektronicznych oraz na pierwszych zajęciach (w każdej formie zajęć).

Treści programowe

Przedmiot „Bezpieczeństwo systemów IoT i IIoT” wprowadza studentów w kluczowe zagadnienia związane z ochroną systemów Internetu Rzeczy (IoT) oraz przemysłowego Internetu Rzeczy (IIoT). Kurs łączy aspekty teoretyczne i praktyczne, pozwalając studentom zrozumieć specyfikę infrastruktury fizycznej, sieciowej i organizacyjnej w środowiskach przemysłowych. Omawia zagrożenia specyficzne dla IoT i IIoT, takie jak ataki na infrastrukturę krytyczną, niezabezpieczone standardy Ethernet oraz problemy wynikające z braku segmentacji sieci. Zajęcia praktyczne obejmują projektowanie i zabezpieczanie systemów IoT, a także analizę rzeczywistych scenariuszy zagrożeń w przemyśle.

Tematyka zajęć

I. Wprowadzenie do bezpieczeństwa systemów IoT i IIoT (6x45 minut)
1. Podstawowe pojęcia i definicje
o Różnice między IoT a IIoT.
o Wymagania i wyzwania bezpieczeństwa w środowiskach przemysłowych.
o Normy i standardy (np. NIS2, IEC 62443).
2. Model Purdue
o Warstwowa architektura systemów przemysłowych.
o Segmentacja i izolacja sieci jako podstawa bezpieczeństwa.
3. Aspekty prawne i organizacyjne
o Wymogi prawne dotyczące ochrony infrastruktury krytycznej.
o Struktura organizacyjna i zespoły bezpieczeństwa.
II. Bezpieczeństwo sprzętowe i platformowe (6x45 minut)
1. Bezpieczeństwo platform IoT
o Analiza bezpieczeństwa urządzeń takich jak Raspberry Pi, Arduino.
o Zabezpieczenia na poziomie sprzętowym.
2. Bezpieczeństwo połączeń sieciowych IoT
o Protokoły komunikacyjne (MQTT, CoAP) i ich zabezpieczenia.
o Ochrona połączeń bezprzewodowych (Wi-Fi, Bluetooth).
o Firewall i systemy IPS w środowiskach IoT i IIoT.
3. Bezpieczeństwo platform chmurowych IoT
o Microsoft Azure, AWS, Google Cloud - analiza zagrożeń i zabezpieczeń.
o Bezpieczne zarządzanie danymi w chmurze.
III. Specyfika bezpieczeństwa w przemyśle (IIoT) (6x45 minut)
1. Bezpieczeństwo sieciowe w przemyśle

o Zagrożenia wynikające z niezabezpieczonych standardów Ethernet.
o Zabezpieczenia w sieciach przemysłowych (MPLS, Carrier Ethernet).
o Zarządzanie ruchem sieciowym i ochrona przed atakami DDoS.
2. Ataki na infrastrukturę krytyczną
o Analiza przykładów ataków na systemy SCADA i inne systemy przemysłowe.
o Mechanizmy ochrony infrastruktury krytycznej.
3. Bezpieczeństwo funkcjonalne i operacyjne
o Zarys bezpieczeństwa funkcjonalnego w przemyśle.
o Zasady bezpieczeństwa pracy w środowiskach przemysłowych.
IV. Zarządzanie cyklem życia systemu IoT i IIoT (6x45 minut)
1. Monitorowanie i aktualizacja systemów IoT/IIoT
o Bezpieczne zarządzanie aktualizacjami urządzeń.
o Zdalne zarządzanie i monitorowanie systemów IoT.
2. Automatyzacja konfiguracji urządzeń sieciowych
o Wprowadzenie do skryptów automatyzujących procesy konfiguracyjne.
o Przykłady narzędzi do automatyzacji w środowiskach IoT i IIoT.
V. Laboratoria i projekt
1. Laboratoria
o Konfiguracja bezpiecznych połączeń IoT i IIoT (np. zabezpieczenie MQTT, CoAP).
o Zastosowanie mechanizmów firewall i IPS w środowiskach IoT.
o Analiza bezpieczeństwa urządzeń Raspberry Pi i Arduino.
2. Projekt grupowy
o Budowa bezpiecznego systemu IoT: analiza zagrożeń, projektowanie architektury, implementacja zabezpieczeń.
o Prezentacja rezultatów i dyskusja nad efektywnością zastosowanych rozwiązań.2. Umiejętności: bieżąca ocena zadań laboratoryjnych oraz ocena końcowa projektu grupowego.

Metody dydaktyczne

• Wykłady z elementami analiz przypadków i prezentacji multimedialnych, online.
• Laboratoria praktyczne z konfiguracji i zabezpieczania urządzeń IoT.
• Praca zespołowa w ramach projektu grupowego.

Literatura

Podstawowa:
1. "IoT Security: Advances in Authentication" - Chintan Patel, Sudhir Rawat. Wiley, 2021. ISBN: 978-1119676687.
2. "Industrial Cybersecurity: Efficiently Secure Critical Infrastructure Systems" - Pascal Ackerman. Elsevier, 2019. ISBN: 978-0128146870. Amazon.
3. NIS2 Directive - Directive (EU) 2022/2555 of the European Parliament and of the Council. Official Journal of the European Union, December 2022. EUR-Lex.
IEC 62443 - Industrial communication networks - Network and system security. International Electrotechnical Commission (IEC), 2020. IEC Standards.

Uzupełniająca:

Materiały dydaktyczne przygotowane przez prowadzących.

Bilans nakładu pracy przeciętnego studenta

	Godzin	ECTS
Łączny nakład pracy	116	4,00
Zajęcia wymagające bezpośredniego kontaktu z nauczycielem	56	2,00
Praca własna studenta (studia literaturowe, przygotowanie do zajęć laboratoryjnych/ćwiczeń, przygotowanie do kolokwiów/egzaminu, wykonanie projektu)	60	2,00