

Cyber-Ochrona Infrastruktury IoT/Ot z Wykorzystaniem AI

Kod przedmiotu: COII

Rodzaj przedmiotu: obieralny

Specjalność: Cyberbezpieczeństwo i AI

Wydział: Informatyki

Kierunek: Informatyka

Poziom studiów: pierwszego stopnia – VI poziom PRK

Profil studiów: praktyczny

Forma studiów: stacjonarna/niestacjonarna

Rok: 3

Semestr: 5

Formy zajęć i liczba godzin:

Forma stacjonarna

- wykłady – 30
- laboratorium – 45

Forma niestacjonarna

- wykłady – 15
- laboratorium – 20

Zajęcia prowadzone są w języku polskim.

Liczba punktów ECTS: 6

Osoby prowadzące:

wykład:

laboratorium:

1. Założenia i cele przedmiotu

Przedmiot skupia się na bezpieczeństwie dynamicznie rosnącego sektora Przemysłu 4.0, inteligentnych miast oraz urządzeń brzegowych (Edge/IoT). Studenci poznają specyfikę środowisk OT (Operational Technology) i SCADA, które wymagają zupełnie innego podejścia do ochrony niż klasyczne sieci IT. Głównym celem kursu jest nauka wdrażania lekkich modeli sztucznej inteligencji bezpośrednio na urządzeniach końcowych (np. Raspberry Pi, mikrokontrolery) w celu autonomicznej detekcji anomalii, zapobiegania tworzeniu botnetów i ochrony infrastruktury krytycznej przed cyber-sabotażem.

2. Określenie przedmiotów wprowadzających wraz z wymaganiami wstępnymi

Wymogi wstępne dotyczą wiedzy i umiejętności z następujących obszarów:

- Znajomość podstawowych koncepcji sieciowych i protokołów komunikacyjnych.
- Podstawy programowania w języku Python oraz C/C++.

- Znajomość systemów operacyjnych z rodziny Linux

3. Opis form zajęć

a) Wykłady

- **Treści programowe:**

1. Architektura IoT i OT: Wprowadzenie do Przemysłu 4.0, systemów SCADA, PLC oraz urządzeń Edge. Główne różnice w podejściu do bezpieczeństwa między IT a OT.
2. Protokoły komunikacyjne w IoT: Analiza bezpieczeństwa protokołów takich jak MQTT, CoAP, Zigbee, LoRaWAN.
3. Krajobraz zagrożeń dla systemów wbudowanych: Analiza historycznych ataków (np. Stuxnet, Mirai botnet). Wektory ataków sprzętowych i sieciowych.
4. Edge AI i TinyML w cyberbezpieczeństwie: Teoria przenoszenia analityki i detekcji zagrożeń na urządzenia brzegowe (Edge computing). Optymalizacja modeli ML do pracy na ograniczonych zasobach.
5. Regulacje i standardy: Wprowadzenie do standardów bezpieczeństwa przemysłowego (np. IEC 62443).

- **Metody dydaktyczne:**

Wykład prowadzony jest w formie prezentacji multimedialnej, uzupełnionej przykładami, analizą przypadków oraz dyskusją nad praktycznymi zastosowaniami prezentowanych treści.

- **Forma i warunki zaliczenia:**

- Warunkiem zaliczenia wykładu jest aktywne uczestnictwo w wykładzie.
- Wykazanie się przedmiotową wiedzą w pracach projektowych.

- **Wykaz literatury podstawowej:**

1. Macaulay, T. (2019). IoT Security: Fundamentals, Techniques, and Strategies.
2. Knapp, E. D., Langill, J. T. (2014). Industrial Network Security: Securing Critical Infrastructure Networks for Smart Grid, SCADA, and Other Industrial Control Systems. Syngress.
3. Oficjalna dokumentacja AWS IoT / Azure IoT.

- **Wykaz literatury uzupełniającej:**

1. Warden, P., Situnayake, D. (2019). TinyML: Machine Learning with TensorFlow Lite on Arduino and Ultra-Low-Power Microcontrollers. O'Reilly Media (w zakresie wdrażania ML na małych urządzeniach).
2. Wytyczne ENISA dotyczące bezpieczeństwa Internetu Rzeczy i infrastruktury krytycznej.

b) *Laboratorium*

- **Treści programowe:**

1. Realizacja praktycznych ćwiczeń laboratoryjnych zgodnych z zakresem przedmiotu.
2. Analiza przypadków i rozwiązywanie problemów praktycznych.
3. Opracowanie projektu końcowego związanego z tematyką przedmiotu.

- **Metody dydaktyczne:**

W trakcie zajęć prowadzący omawia zagadnienia związane z realizacją poszczególnych ćwiczeń, a następnie studenci samodzielnie lub zespołowo realizują zadania określone przez prowadzącego.

• **Forma i warunki zaliczenia:**

Warunkiem zaliczenia jest uczestnictwo w zajęciach, wykonanie ćwiczeń laboratoryjnych, przygotowanie projektu końcowego.

- **Wykaz literatury podstawowej:**
 - Jak w przypadku wykładu.
- **Wykaz literatury uzupełniającej:**
 - Jak w przypadku wykładu.

4. Opis sposobu wyznaczania punktów ECTS

a. forma stacjonarna

Forma zajęć	Formy aktywności studenta	Średnia liczba godzin na zrealizowanie aktywności
Wykład	Kontakt z nauczycielem	30
	Czytanie wskazanej literatury	10
	Przygotowanie do egzaminu	10
Laboratorium	Kontakt z nauczycielem	45
	Czytanie wskazanej literatury	10
	Wykonanie zadań laboratoryjnych	19
	Przygotowanie projektu	20
Konsultacje	Kontakt z nauczycielem	3
Zal./Egzamin	Kontakt z nauczycielem	3
Całkowita ilość godzin aktywności studenta		150
Liczba punktów ECTS dla modułu/przedmiotu		6

a. forma niestacjonarna

Forma zajęć	Formy aktywności studenta	Średnia liczba godzin na zrealizowanie aktywności
Wykład	Kontakt z nauczycielem	15
	Czytanie wskazanej literatury	15
	Przygotowanie do egzaminu	20
Laboratorium	Kontakt z nauczycielem	20
	Czytanie wskazanej literatury	24
	Wykonanie zadań laboratoryjnych	20
	Przygotowanie projektu	30
Konsultacje	Kontakt z nauczycielem	3
Zal./Egzamin	Kontakt z nauczycielem	3
Całkowita ilość godzin aktywności studenta		150
Liczba punktów ECTS dla modułu/przedmiotu		6

5. Wskaźniki sumaryczne

a. forma stacjonarna

- liczba godzin dydaktycznych (tzw. kontaktowych) i liczba punktów ECTS na zajęciach wymagających bezpośredniego udziału nauczycieli akademickich
 - Liczba godzin kontaktowych – 81
 - Liczba punktów ECTS – 3,2
- liczba godzin dydaktycznych (tzw. kontaktowych) i liczba punktów ECTS na zajęciach o charakterze praktycznym.
 - Liczba godzin kontaktowych – 45
 - Liczba punktów ECTS – 3,8

b. forma niestacjonarna

- a) liczba godzin dydaktycznych (tzw. kontaktowych) i liczba punktów ECTS na zajęciach wymagających bezpośredniego udziału nauczycieli akademickich
 - Liczba godzin kontaktowych – 41
 - Liczba punktów ECTS – 1,6
- b) liczba godzin dydaktycznych (tzw. kontaktowych) i liczba punktów ECTS na zajęciach o charakterze praktycznym.
 - Liczba godzin kontaktowych – 20

Liczba punktów ECTS – 3,8

6. Zakładane efekty uczenia się

Efekt przedmiotowy (Symbol)	Efekty uczenia się dla przedmiotu	Odniesienie do kierunkowych efektów uczenia się
COII_01	... Zna specyfikę infrastruktury krytycznej, protokołów komunikacyjnych IoT/OT oraz wektorów ataków celujących w systemy wbudowane.	K_W04, K_W09
COII_02	... Potrafi skonfigurować bezpieczną komunikację dla urządzeń brzegowych, w tym zastosować szyfrowanie i segmentację sieci dla IoT.	K_U02, K_U11
COII_03	... Umie wdrożyć lekki model sztucznej inteligencji na urządzeniu typu Edge w celu monitorowania zachowania i blokowania anomalii.	K_U02, K_U11
COII_04	... Ma świadomość fizycznych, gospodarczych i społecznych konsekwencji cyberataków na infrastrukturę przemysłową (OT) i potrafi krytycznie oceniać ryzyko.	K_U23, K_K03

7. Odniesienie efektów uczenia się do form zajęć i sposób oceny osiągnięcia przez studenta efektów uczenia się

Efekt przedmiotowy (Symbol)	Forma zajęć		Sposób sprawdzenia osiągnięcia efektu
	Wykład	Laboratorium	
COII_01	<i>x</i>		Potrafi wykorzystać wiedzę z zakresu przedmiotu w pracach projektowych
COII_02	<i>x</i>	<i>x</i>	Potrafi wykorzystać wiedzę z zakresu przedmiotu w pracach projektowych, dyskusja na zajęciach, sprawozdanie z projektu, zadania praktyczne
COII_03		<i>x</i>	dyskusja na zajęciach, sprawozdanie z projektu, zadania praktyczne
COII_04		<i>x</i>	dyskusja na zajęciach, sprawozdanie z projektu, zadania praktyczne

8. Kryteria uznania osiągnięcia przez studenta efektów uczenia się

Efekt	Efekt jest uznawany za osiągnięty gdy:
COII_01	Projekt spełnia założone wymagania Poprawnie wykonuje zadania w czasie zajęć. Potrafi objaśnić elementy projektu
COII_02	Projekt spełnia założone wymagania Poprawnie wykonuje zadania w czasie zajęć. Potrafi objaśnić elementy projektu
COII_03	Projekt spełnia założone wymagania Poprawnie wykonuje zadania w czasie zajęć. Potrafi objaśnić elementy projektu
COII_04	Projekt spełnia założone wymagania Poprawnie wykonuje zadania w czasie zajęć. Potrafi objaśnić elementy projektu