KARTA OPISU PRZEDMIOTU - SYLABUS

Nazwa przedmiotu
Wykrywanie anomalii sieciowych i detekcja zagrożeń w sieci z wykorzystaniem AI [S1Cybez1>WAS]

Przedmiot

Kierunek studiów
Cyberbezpieczeństwo

Rok/Semestr
3/6

Studia w zakresie (specjalność)
–

Profil studiów
ogólnoakademicki

Poziom studiów
pierwszego stopnia

Język oferowanego przedmiotu
polski

Forma studiów
stacjonarne

Wymagalność
obieralny

Liczba godzin

Wykład
16

Laboratorium
30

Inne
0

Ćwiczenia
0

Projekty/seminaria
12

Liczba punktów ECTS

4,00

Koordynatorzy

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

dr Joanna Weissenberg
joanna.weissenberg@put.poznan.pl

Wykładowcy

Wymagania wstępne

Podstawy lokalnych i rozległych sieci komputerowych

Cel przedmiotu

• Zapoznanie studentów z metodami monitorowania sieci i identyfikacji urządzeń w środowisku sieciowym. • Wprowadzenie do algorytmów sztucznej inteligencji stosowanych w analizie ruchu sieciowego. • Rozwinięcie praktycznych umiejętności implementacji systemów detekcji zagrożeń. • Przygotowanie do projektowania i wdrażania nowoczesnych rozwiązań ochrony sieci komputerowych.

Przedmiotowe efekty uczenia się

Wiedza:
• Student zna podstawowe techniki identyfikacji urządzeń w sieci i monitorowania ruchu sieciowego. [K1_W07]
• Rozumie algorytmy AI wykorzystywane w analizie sieci i detekcji zagrożeń. [K1_W16]

• Posiada wiedzę na temat systemów oraz narzędzi analizy ruchu sieciowego. [K1_W07]

Umiejętności:
• Potrafi monitorować sieć i identyfikować anomalie w ruchu sieciowym. [K1_U04]
• Umie implementować modele AI do wykrywania zagrożeń w sieciach komputerowych. [K1_U05]
• Jest w stanie zaprojektować i wdrożyć system ochrony sieci oparty na AI. [K1_U03]

Kompetencje społeczne:
• Rozumie znaczenie rozwoju technologii AI w kontekście bezpieczeństwa sieciowego. [K1_K01]
• Potrafi pracować w grupie nad złożonymi projektami technologicznymi. [K1_K05]
• Jest świadomy odpowiedzialności za wdrażanie rozwiązań zapewniających bezpieczeństwo sieci. [K1_K05]

Metody weryfikacji efektów uczenia się i kryteria oceny

Efekty uczenia się przedstawione wyżej weryfikowane są w następujący sposób:

1. Wiedza: egzamin pisemny lub ustny sprawdzający znajomość technik monitorowania sieci i algorytmów AI.
2. Umiejętności: bieżąca ocena realizacji zadań laboratoryjnych.
3. Projekt: ocena końcowa na podstawie implementacji, dokumentacji i prezentacji systemu detekcji zagrożeń.
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 „Wykrywanie anomalii sieciowych i detekcja zagrożeń w sieci z wykorzystaniem AI” wprowadza studentów do zaawansowanych technik monitorowania sieci, analizy ruchu oraz wykrywania zagrożeń z wykorzystaniem sztucznej inteligencji. Obejmuje tworzenie odcisków palców urządzeń sieciowych, nadzór nad ich funkcjonowaniem oraz implementację algorytmów AI do analizy ruchu sieciowego, identyfikacji anomalii i wykrywania ataków. Zajęcia teoretyczne i praktyczne rozwijają wiedzę oraz umiejętności potrzebne do projektowania i wdrażania systemów monitorowania i ochrony sieci.

Tematyka zajęć

I. Wprowadzenie do monitorowania sieci i wykrywania zagrożeń (8x45 min)
1. Podstawowe pojęcia i technologie
o Automatyczna klasyfikacja urządzeń sieciowych
o Jednoznaczna identyfikacja urządzeń w sieci i tworzenie ich odcisków palców.
o Rola monitorowania sieci w zapewnianiu bezpieczeństwa.
o Wprowadzenie do analizy ruchu sieciowego.
2. Architektura i narzędzia monitorowania sieci
o Przegląd narzędzi i systemów do analizy ruchu sieciowego
o Metryki i wskaźniki monitorowania sieci.
II. Detekcja anomalii w sieciach komputerowych (8x45 min)
1. Techniki wykrywania anomalii
o Klasyfikacja anomalii: anomalie ilościowe, jakościowe i czasowe.
o Analiza ruchu sieciowego pod kątem odchyleń od normy.
2. Wykrywanie zagrożeń z wykorzystaniem sztucznej inteligencji
o Algorytmy uczenia maszynowego i ich zastosowanie w analizie ruchu sieciowego
o Wprowadzenie do uczenia głębokiego (Deep Learning) w analizie ruchu sieciowego.
o Przykłady wykorzystania AI w detekcji ataków sieciowych (np. DDoS, phishing).
III. Implementacja systemów ochrony z wykorzystaniem AI (8x45 min)
1. Projektowanie systemów detekcji zagrożeń
o Proces budowy modelu AI do analizy sieci.

o Zbieranie danych, etykietowanie i przygotowanie zbiorów treningowych.
o Walidacja i testowanie modeli wykrywających anomalie.
2. Zarządzanie urządzeniami w sieci
o Monitorowanie wykorzystania zasobów urządzeń (CPU, pamięć, pasmo).
o Integracja algorytmów AI z istniejącymi systemami sieciowymi.
3. Zarządzanie komunikacją maszyna-maszyna w zakresie automatyzacji przekazywania informacji o IoC i IoA
o STIX
o TAXII
IV. Laboratoria i projekt grupowy
1. Laboratoria praktyczne
o Tworzenie odcisków palców urządzeń w sieci i ich analiza.
o Wykorzystanie narzędzi do analizy ruchu sieciowego i identyfikacji anomalii.
o Implementacja podstawowych algorytmów AI do detekcji zagrożeń.
2. Projekt grupowy
o Opracowanie i wdrożenie systemu wykrywania zagrożeń z wykorzystaniem AI.
o Analiza danych, implementacja algorytmów i prezentacja wyników.

Metody dydaktyczne

• Wykłady z prezentacją multimedialną i przykładami praktycznymi.
• Laboratoria obejmujące konfigurację narzędzi analizy sieci i implementację algorytmów AI.
• Projekty grupowe, polegające na opracowaniu kompleksowego systemu detekcji zagrożeń.

Literatura

Podstawowa:
• "Artificial Intelligence for Cybersecurity" by Mark Stamp:
Stamp, M., Visaggio, C. A., Mercaldo, F., & Di Troia, F. (Eds.). (2022). Artificial Intelligence for Cybersecurity. Springer International Publishing.
amazon.com
• Dokumentacja narzędzi analizy sieci (e.g., Wireshark, Zeek):
• Wireshark: Wireshark Foundation. (n.d.). Wireshark User Guide. Retrieved from https://www.wireshark.org/docs/wsug_html_chunked/
• Zeek (formerly known as Bro): Zeek Project. (n.d.). Zeek Documentation. Retrieved from https://docs.zeek.org/en/stable/

Uzupełniająca:
1. Materiały dydaktyczne przygotowane przez prowadzących.

Bilans nakładu pracy przeciętnego studenta

	Godzin	ECTS
Łączny nakład pracy	103	4,00
Zajęcia wymagające bezpośredniego kontaktu z nauczycielem	58	2,50
Praca własna studenta (studia literaturowe, przygotowanie do zajęć laboratoryjnych/ćwiczeń, przygotowanie do kolokwiów/egzaminu, wykonanie projektu)	45	1,50